Ο HACKER

Season 05 / Issue 09

τεύχος 057 - Norðurfjörður Edition



Πρακτικές κρυπτογράφησης δεδομένων στο δίσκο [*]

Το δικό σας openSUSE, αλλά στο cloud

Ο Apache με έγκυρο πιστοποιητικό, στο Raspberry Pi στο σπίτι

Ομαλή αναβάθμιση στο Leap 42.2, από τη γραμμή εντολών

Διαχείριση κατατμήσεων με το GParted

[*] και χάστε το laptop σας χωρίς άγχος

all rights reversed

HACKER


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

#dH057 | Περιεχόμενα

Εκδότης / Διευθυντής	Χρήστος Βαρελάς
Αρχισυντάκτης	Παναγιώτης Βαρελάς
Σύμβουλοι έκδοσης	Νίκος Μουρατίδης, Βούλα Παυλίδου
Σύνταξη	Παναγιώτης Βαρελάς, Χρήστος Βαρελάς, Πάνος Γεωργιάδης, Γιώργος Γιάννου, Μάριος Καραγιαννόπουλος, Γιάννης Κρομμύδας, Πέτρος Κυλαδίτης, Μέσος Παπαδόπουλος (TM), Χρίστος Τόμπρας, @arkoudos
Γραμματική επιμέλεια	Βούλα Παυλίδου
Καλλιτεχνική Επιμέλεια	Πέτρος Φιλιππίδης

Το ψηφιακό περιοδικό deltaHacker είναι συνδρομητικό και εκδίδεται από την Parabing Creations. Ο δικτυακός τόπος του περιοδικού είναι στο https://deltahacker.gr και το email επικοινωνίας είναι το talk2us@deltahacker.gr. Οι γενικές πληροφορίες για τις συνδρομές παρατίθενται στο https://deltahacker.gr/order κι από την ίδια σελίδα γίνονται οι παραγγελίες.

Μικρόκοσμος

του Χρήστου Βαρελά

Φίλες και φίλοι,

- Πέρυσι τέτοιες μέρες ήμουν προβληματισμένος.
- Μη φανταστείτε ότι με απασχολούσε κάτι που ο Μέσος Παπαδόπουλος™ δικαίως θα χαρακτήριζε ως σοβαρό ζήτημα.
- Για το μικρόκοσμό μου, ωστόσο, αυτό που με απασχολούσε δεν ήταν κι εντελώς ασήμαντο.
- Ζούσα ένα μίνι δράμα και, όλως τυχαίως, τις μέρες γύρω από την Πρωτοχρονιά του 2016 βρισκόμασταν με την κα Σύμβουλο Εκδόσεως (TM) στη δροσερή Δράμα.
- Το laptop που είχα αγοράσει μερικές μέρες πριν το περήφανο δημοψήφισμα του 2015, ακόμη έτρεχε το OS X το Yosemity. Αυτό από μόνο του δεν θα ήταν τραγικό ως γεγονός, αν δεν είχε ήδη κυκλοφορήσει το El Capitan από το φθινόπωρο.
- Είχα ενδοιασμούς για το πέρασμα στο El Capitan, τους οποίους μάλιστα τη δεύτερη μέρα του 2016 εξέφρασα και σε σχετικό post που διάβασαν δεκαεννέα επισκέπτες του προσωπικού μου site.
- Προσέξτε: Δεν λέω ότι επισκέπτονται το προσωπικό μου site περισσότεροι από δεκαεννέα άνθρωποι ανά μήνα αλλά έτυχε και μόνο δεκαεννέα διάβασαν το προαναφερθέν post. Λέω ότι *όλοι* οι επισκέπτες του προσωπικού μου site διάβασαν το προαναφερθέν post.
- Μικρό νούμερο, αλλά όχι για τον μικρόκοσμό μου.
- Τέλος πάντων, περίπου 350 μέρες πέρασαν κι αυτή τη φορά καθόλου δεν προβληματίστηκα που, ενώ είχε βγει το Sierra από το φθινόπωρο, το laptop μέχρι πρότινος ακόμη έτρεχε το El Capitan.
- Για να είμαι ειλικρινής, δεν πρόλαβα καν να προβληματιστώ. Όχι ότι μου συνέβη κάτι κι άλλαξα ως άνθρωπος κι άρχισαν να μ' απασχολούν πιο σοβαρά και σπουδαία ζητήματα. Απλά, λίγες μέρες πριν ξεκίνησα τη διαδικασία αναβάθμισης κατά λάθος.

- Κατά λάθος λόγω αφηρημάδας, για να είμαι ακριβής.
- Καιρό έβλεπα την ειδοποίηση περί διαθέσιμων αναβαθμίσεων να εμφανίζεται πάνω δεξιά στην οθόνη. Είχα τσεκάρει και διαπιστώσει ότι, πράγματι, μία από τις αναβαθμίσεις αφορούσε στο ίδιο το λειτουργικό σύστημα. Κάποια στιγμή μάλιστα είχα κάνει και κλικ στο κουμπάκι κάτω από τη σχετική ειδοποίηση, στο App Store. Το σκεπτικό μου ήταν να δω πόσο μεγάλο είναι το update για το Sierra και ίσως να κατέβαζα ένα μέρος του, ώστε αργότερα η λήψη και η αναβάθμιση να ολοκληρωθούν γρηγορότερα.
- Γύρω στα τεσσεράμισι gigabyte ήταν το μέγεθος του update για το Sierra, που λέτε, και την πρώτη φορά άφησα να κατέβουν κοντά στα τριακόσια megabyte πριν διακόψω τη διαδικασία.
- Λίγες μέρες πριν, χωρίς να υπάρχει κάποιος ιδιαίτερος λόγος, μου 'ρθε να κατεβάσω λίγο ακόμα από το update.
- Είναι φοβερή η πρόοδος που έχουμε κάνει, ως ανθρωπότητα. Σκεφτείτε το: Έχουμε φτάσει σε τόσο υψηλό επίπεδο αφαίρεσης, ώστε η φράση "να κατεβάσω λίγο ακόμα από το update" σχεδόν βγάζει νόημα. Εκπληκτικά πράγματα.
- Τέλος πάντων, πήγα ξανά στο App Store, πάτησα στο κουμπάκι, σηκώθηκα από το γραφείο, έπιασα κάτι δουλειές του σπιτιού που αμελούσα.
- Το έχω παρατηρήσει: Ένα καλό κόλπο για να σταματάω ν' αναβάλω βαρετές δουλειές και να τους επιτίθεμαι απότομα, είναι να βάζω τον υπολογιστή να κάνει κάτι – οτιδήποτε. Σκέφτομαι έτσι ότι ο χρόνος που ξοδεύω για τις βαρετές δουλειές δεν πηγαίνει πέρα για πέρα χαμένος.
- Παράξενο, το ξέρω. Στοιχηματίζω όμως ότι καταλαβαίνετε πολύ καλά για τι πράγμα μιλάω.
- Καθώς έκανα δουλειές, ήσυχος με την ιδέα ότι ούτε το laptop κάθεται, άρχισα να σκέφτομαι πόσο τρόμπες –ναι, σωστά διαβάσατε, τρόμπες– είναι κάποιοι εκεί στο Facebook, που θεωρούν εξ ορισμού κακόβουλα τα domains με κατάληξη ".xyz".
- Και δεν είναι ότι τα θεωρούν εξ ορισμού κακόβουλα, σκιάζουν κι όσους τολμούν να κάνουν κλικ πάνω τους. Στο δε Instagram η κατάσταση είναι χειρότερη, αφού εκτός από τη δυσοίωνη προειδοποίηση το URL δεν είναι καν clickable.

- Αλλά δεν με νοιάζει. Δεν θα αλλάξω εγώ το ωραιότατο colder.xyz, επειδή α) κάποιοι έχουν πράγματι κακόβουλα sites με κατάληξη ".xyz" και β) το Facebook θέλει σώνει και καλά να μας παριστάνει τον προστάτη.
- Όχι. Θα συνεχίσω να γράφω στο colder.xyz ό,τι μου 'ρχεται (as in "αραιά και πού"), ενώ ταυτόχρονα θα χρησιμοποιώ και subdomains του colder.xyz για άλλα πρότζεκτ.
- Εδώ και μερικές βδομάδες, για παράδειγμα, παίζω μ' ένα καινούργιο Raspberry Pi 3. Όπου να 'ναι θα εγκαταστήσω εκεί το NextCloud, τον διάδοχο του ownCloud. Το NextCloud θα αποτελέσει μέρος μιας γενικότερης στρατηγικής backup που σχεδιάζω τον τελευταίο καιρό. Αλλά ας μην ξεφεύγω, αυτά δεν είναι του παρόντος. Ως web server για το NextCloud έχω επιλέξει τον Apache, ο οποίος ήδη τρέχει στο RasPi. Κάποια στιγμή συνειδητοποίησα ότι, από τη στιγμή που έχω πλήρη έλεγχο στον name server του colder.xyz, μπορώ να έχω και δωρεάν πιστοποιητικό για ένα οποιοδήποτε subdomain του. Θα φτάνω έτσι στο site που σερβίρει ο Apache, από το RasPi στο σπίτι, χωρίς να ξέρω το δημόσιο IP του modem/router μπροστά από τη συσκευή και χωρίς να παίρνω προειδοποιήσεις για self-signed πιστοποιητικά και τα ρέστα.
- Κάτι τέτοια σκεφτόμουν και χωρίς να το καταλάβω τελείωσα με τις βαρετές δουλειές – χωρίς να βαρεθώ καθόλου.
- Πήγα στο laptop, να δω πού είχε φτάσει το download του Sierra και να το σταματήσω.
- Δεν χρειάστηκε.
- Το Sierra είχε κατέβει κι ο σχετικός installer είχε ενεργοποιηθεί, περιμένοντας ένα κλικ στο κουμπάκι Next ώστε να προχωρήσει στην αναβάθμιση του λειτουργικού. Τώρα που το σκέφτομαι, δεν θυμάμαι αν υπήρχε κουμπάκι Next ή κάποια θυρίδα για το password του administrator. Όπως και να ήταν, δεν μου πήγε η καρδιά να σταματήσω τη διαδικασία.
- Περίπου μισή ώρα αργότερα το El Capitan αποτελούσε παρελθόν και το Sierra έδειχνε να δουλεύει μια χαρά. Χρειάστηκε μόνο να εγκαταστήσω εκ νέου το MacPorts, ενώ διαπίστωσα ότι και τα GPG Tools δεν είναι ακόμη έτοιμα για το Mail του Sierra. Πρακτικά, αυτό το τελευταίο σημαίνει ότι προς το παρόν δεν μπορώ να διαβάζω *εύκολα* emails που έχουν κρυπτογραφηθεί με το δημόσιο κλειδί μου.

/var/log/messages

- Είναι νομίζω ασφαλές να υποθέσουμε ότι το ποσοστό των ανθρώπων στον πλανήτη οι οποίοι κρυπτογραφούν τα εξερχόμενα emails με τα δημόσια κλειδιά των παραληπτών, εκφράζεται από το μηδέν ακολουθούμενο από υποδιαστολή, αρκετά μηδενικά και μετά δύο μη-μηδενικά ψηφία.
- Στον μικρόκοσμό μου λείπουν μερικά μηδενικά μετά την υποδιαστολή, όχι όμως τόσα πολλά ώστε ν' ανησυχώ ιδιαίτερα.
- Όλα καλά λοιπόν με την αναβάθμιση στο Sierra και πολύ χαίρομαι γι' αυτό, αφού τώρα μπορώ να στρέψω την προσοχή μου σε άλλα παντελώς ασήμαντα για την ανθρωπότητα θέματα, αρκετά σημαντικά όμως για 'μένα. Α, και μη νομίζετε ότι μιλάω γενικά κι αόριστα. Σας αναφέρω μερικά μόνο από τα items (έτσι τα λέω) της σχετικής λίστας που συντηρώ:
    - Λεπτομερές demo επίθεσης privilege escalation, το οποίο εκμεταλλεύεται ύπουλη αδυναμία της MariaDB. Πρόκειται για άρθρο που κατά 98,7% θα δημοσιευτεί στο επόμενο τεύχος του deltaHacker, το υπ' αριθμόν 058.
    - Νέο static site που βασίζεται στο Hugo και τελεί υπό τον έλεγχο του Git. Προσωπικό πρότζεκτ, μάλλον θ' αποτελέσει κι αυτό αφορμή για άρθρο στο 058.
    - Παρουσίαση και χρήση του i3 WM, για *αληθινά* macho supremo χρήστες του Linux. Ναι, κι αυτό θα γίνει άρθρο στο περιοδικό, αλλά μάλλον όχι στο 058.
    - Το BtrFS και το snapper, μυστικά του zypper, το τιτάνιο tmux, το Mathematica στο Raspberry Pi (δεν μιλάω μόνο για εγκατάσταση), το υπερεργαλείο διαχείρισης πολλών (απομακρυσμένων) συστημάτων ονόματι Salt κ.ο.κ.
- Νομίζω ότι εδώ μπορεί να μπει μια άνω τελεία.
- Καλή σας ανάγνωση, καλή χρονιά να έχουμε, καλά να είμαστε και να φτιάχνουμε ωραίους μικρόκοσμους.
- Όχι κατ' ανάγκη απομονωμένους από άλλους κόσμους τριγύρω, μικρούς ή μεγαλύτερους.



σνέιλ μέιλ

Αγαπητοί μου,

Έψαχνα να βρω τη λέξη εκείνη που θα περιέγραφε καλύτερα το πώς νοιώθω τώρα που τελειώνει το 2016.

Αμφιθυμία. Αυτή είναι η λέξη.

Από την μία είμαι καταχαρούμενος που τελειώνει. Να πάει από εκεί που ήρθε και να μην ξανάρθει.

Κι από την άλλη με πιάνει σύγκρυο όταν συνειδητοποιώ πως ναι μεν το 2016 τελειώνει, αλλά καταφτάνει το 2016++.

Αν νομίζει κανείς πως θα τη βγάλουμε καθαρή κάνει μεγάλο λάθος, αγαπητοί μου, αλλά δεν θα σας απασχολήσω με αυτά σήμερα. Έχουμε καιρό να τα πούμε και δε νομίζω πως περιμένατε εμένα και τις επιστολές μου για να σχηματίσετε γνώμη.

Σήμερα θα ήθελα να πιάσω το ζήτημα της μνήμης -- της ανθρώπινης, όχι της κομπιουτερικής. Ατομικής αλλά και συλλογικής· μνήμης αλλά και λήθης.

Είναι ένα ζήτημα που όσο το σκέφτομαι, τόσο πιο πολύπλοκο μου μοιάζει.

Θα μου πείτε, κομπιούτορες άνθρωποι, ποια η δυσκολία; Αφού ξέρουμε τι είναι η μνήμη. Δεν ξέρουμε; Δεν είναι ο αποθηκευτικός εκείνος χώρος στον οποίο καταγράφονται όλα τα δεδομένα που μας αφορούν, εμπειρίες, γνώσεις, γεγονότα, σκέψεις κ.λπ., συνυφασμένος με έναν μηχανισμό ανάκλησης που μας δίνει πρόσβαση στα δεδομένα αυτά; Κάτι σαν RAM, δηλαδή, ή σαν σκληρός δίσκος; Όχι;

Όχι. Δεν είναι τόσο απλό.

Όπως αρμόζει σε τέτοια προβλήματα, ας ξεκινήσουμε από τους ορισμούς.

Ας πάρουμε ως υπόθεση εργασίας πως τόσο στους κομπιούτορες, όσο και στους ανθρώπους ή τις γάτες, μνήμη είναι πράγματι ο μηχανισμός που επιτρέπει την καταγραφή "δεδομένων" σε κάποιο μέσο, καθώς και τη μεταγενέστερη ανάκλησή τους κατά βούληση.

Ερώτησις.

Πώς ακριβώς κατανοούμε τον όρο "δεδομένο"; Πώς ορίζουμε το "δεδομένο"; Ποια είναι η στοιχειώδης μονάδα δεδομένων στην ανθρώπινη μνήμη; Ή έστω στη γατίσια μνήμη; Στους υπολογιστάδες είναι το bit. Στους ανθρώπους;

Σκέφτεται ο επιστήμων, απαντάει. Bit και πάλι. Οι νευρώνες είναι ψηφιακοί, κ.λπ. κ.λπ. κ.λπ. Άρα bit.

Τα μετρήσανε κιόλας, διάβαζα κάπου. Τι βρήκανε; 2,5 Petabyte βρήκανε. Ήτοι δυόμιση εκατομμύρια γιγαμπάιτ. Η χωρητικότητα του εγκεφάλου.

Ναι, κι εγώ μέτρησα τον ουρανό με τ' άστρα. Και τι βρήκα; Μια τρύπα στο νερό βρήκα.

Έστω πως η ανθρώπινη μνήμη είναι παρόμοια με αυτή των πληροφορικών συστημάτων, κι έστω πως μετριέται σε bit: Πώς εξηγούμε τότε την απλή παρατήρηση ότι δεν συμπεριφέρεται καθόλου σαν τέτοια; Μα καθόλου;

Έρχεται ας πούμε τις προάλλες ο ανιψιός και μου δείχνει το καινούργιο του διαβατήριο. Το βλέπω. Το πιάνω στα χέρια μου. Το μυρίζω. Κοιτάζω τη φωτογραφία καλά καλά. Γελάω λίγο. Κοιτάζω την ημερομηνία λήξης.

Σνέιλ μέιλ

ΟΚ. Ας προσπαθήσω τώρα να ανακαλέσω το συμβάν. Όλα αυτά που σας είπα τα θυμάμαι. Τα ανακαλώ αυτή τη στιγμή που σας γράφω. Ανακαλώ ξεκάθαρα το να πιάνω το διαβατήριο, να το ξεφυλλίζω, να νοιώθω στα δάχτυλα πόσο δύσκαμπτο είναι, καθώς καινούργιο. Για ρωτήστε με, θυμάμαι την ημερομηνία λήξης; Τον αριθμό;

Φυσικά και δεν τα θυμάμαι. Και δεν είναι πως έχω πρόβλημα μνήμης. Έχω, αλλά δεν είναι αυτό.

Είναι πως οι άνθρωποι τέτοια πράγματα συνήθως δεν τα θυμούνται. Όσους μπορούν και τα θυμούνται τους θαυμάζουμε: "Πω πω, έχει φωτογραφική μνήμη!", λέμε. Εγώ μπορεί να μη θυμάμαι τον αριθμό, αλλά θυμάμαι πώς μυρίζει. Πιάνει αυτό; Και πόσα bit χρειάζονται;

Τη βλέπετε λοιπόν την αντίφαση; Από τη μία θεωρούμε δεδομένο πως η μνήμη μας, η ανθρώπινη μνήμη, είναι με κάποιον τρόπο σαν του κομπιούτορα, κι από την άλλη δεν μας εκπλήσσει καθόλου πως δεν έχει κανένα από τα χαρακτηριστικά που θα περίμενε κανείς να έχει μια τέτοια μνήμη, όπως, π.χ., ακρίβεια, σταθερότητα, ορισμένο μέγεθος, προσβασιμότητα, ταχύτητα και δεν ξέρω τι άλλο.

Γιατί επιμένουμε;

Να σας πω γιατί: Γιατί η ερμηνεία μάς είναι βολική. Γιατί αντικατοπτρίζει το πώς έχουμε μάθει να καταλαβαίνουμε το πώς κινούμαστε στον κόσμο.

Προσέξτε τη διατύπωση. Δεν έγραψα "αντικατοπτρίζει το πώς κινούμαστε στον κόσμο" αλλά ότι "αντικατοπτρίζει το πώς έχουμε συνηθίσει να καταλαβαίνουμε το πώς κινούμαστε στον κόσμο".

Γενικεύοντας: Η εκάστοτε ερμηνεία μας αντικατοπτρίζει το εκάστοτε τρέχον paradigm -- ή "παράδειγμα". Σήμερα αντιλαμβανόμαστε τη μνήμη με όρους πληροφορικών συστημάτων. Πιο παλιά με όρους βιβλίων και ραφιών με βιβλία. Ακόμα πιο παλιά αλλιώς. Στην ουσία, όλον αυτόν τον καιρό παραμένουμε σε άγνοια.

Αυτό ισχυρίζομαι. Πώς δεν έχουμε ιδέα για το πώς λειτουργεί η ανθρώπινη μνήμη και πως αντί να βάλουμε το νιονιό μας να σκεφτούμε, εισάγουμε μοντέλα από άσχετες επιστήμες όπως αυτή των κομπιουτόρων. Και μετά ψάχνουμε να βρούμε γιατί κάτι δεν κολλάει.

Ας πάμε στην άλλη πλευρά του ζητήματος. Στη συλλογική μνήμη (ή καλύτερα στη συλλογική αμνησία).

Ποια είναι η φύση του μηχανισμού που μας επιτρέπει, σε ανθρώπους και κοινωνίες, να ξεχνάμε;

Και πάλι, ας ξεκινήσουμε από τα φαινόμενα. Κυρίως αναφορικά με τις κοινωνίες. Ιδού μερικές από τις σκέψεις μου.

Ανά πάσα στιγμή τα δεδομένα της εκάστοτε επικαιρότητας μας απασχολούν έντονα και επιτακτικά. Μετά περνούν σε δεύτερη μοίρα.

Αυτή η διαδικασία (της αλλαγής προτεραιότητας) δεν γίνεται αυτόματα.

Τα πράγματα δεν φεύγουν από τη συλλογική μνήμη από την μία μέρα στην άλλη. Δεν ξέρω καν αν καταφέρνουν ποτέ να φύγουν εντελώς. Αλλάζουν, παραμορφώνονται, αλλά νομίζω πως δεν φεύγουν.

Στην αρχή τα πράγματα είναι ακόμα ζωντανά. Σπαρταρούν. Χρειάζεται να περάσει καιρός. Χρόνια. Ακόμα και 10 με 15 χρόνια. Εν τέλει τα πράγματα αρχίζουν και ξεθωριάζουν.

Αρχίζουμε από "κάτι", από ένα "συμβάν" που όλοι το "ξέρουμε". Μετά από 15 χρόνια, όμως, ο καθένας μας θυμάται κάτι διαφορετικό. Το περίγραμμα του αρχικού συμβάντος γίνεται όλο και πιο ασαφές. Αυτό που θυμόμασταν τόσο καθαρά, αρχίζει σταδιακά και δίνει τη θέση του σε μια περιγραφή του περί τίνος επρόκειτο. Η αλλαγή αυτή είναι αδιόρατη αλλά συνεχής.



Μέσα σε 30-35 χρόνια έχουν ξεχαστεί όχι μόνο το ίδιο το συμβάν και οι λόγοι που το είχαν καταστήσει επίκαιρο, αλλά και οι διαφορετικοί βαθμοί ασάφειας με τους οποίους το ανακαλούσαν όσοι ακόμα το θυμόντουσαν μέχρι κάποια στιγμή. Μένουν μόνο οι περιγραφές.

Μετά από τριάντα χρόνια, το αρχικό συμβάν, το κάθε συμβάν, έχει αντικατασταθεί από μια περιγραφή του τι υπήρξαν κάποτε αυτά τα συμβάντα.

Μετά από τριάντα χρόνια δεν σκεφτόμαστε πλέον μόνο του το αρχικό συμβάν που κάποτε

είχε λάβει χώρα, αλλά βάζουμε μαζί όλα τα άλλα διάφορα συμβάντα της ίδιας εποχής. Η συζήτηση για το συμβάν γίνεται συζήτηση για την εποχή που έλαβε χώρα το συμβάν. Εποχή που συζητούμε για το αν ήταν ηρωική, ή πανέμορφη, ή τερατώδης, ή τραγική, ή προδοτική, ή ντροπιαστική, ή κακόγουστη, ή ό,τι άλλο τέλος πάντων.

Πρόκειται για μια συζήτηση που έχει λίγη ως ελάχιστη σχέση με το αρχικό "κάτι" και είναι πλέον αξιολογική.

Και τότε γίνεται το εξής ενδιαφέρον: Από τη στιγμή που υπεισέρχονται αξιολογικοί όροι, ξεχωρίζουν και στρατόπεδα. Οι μεν και οι δε. Οι Πράσινοι και οι Βένετοι.

Φυσικά και δεν επρόκειτο ποτέ να συμφωνήσουμε όλοι στο πώς σκεφτόμαστε το ένα ή το άλλο συμβάν ή τη μία ή την άλλη εποχή. Ενώ όμως στην αρχή υπήρχαν τόσες διαφωνίες, όσοι περίπου ήμασταν εμείς που το θυμόμασταν, μετά από τα 30-35 χρόνια οι επί μέρους διαφορές ξεθωριάζουν και καταλήγουμε οι μισοί να το θυμόμαστε μαύρο και οι άλλοι μισοί άσπρο.

Παράδειγμα; Λέμε σήμερα για τη δεκαετία του 80. Μέχρι και έκθεση θα διοργανωθεί στην Τεχνόπολη. Η δεκαετία του 80, η σημαντική δεκαετία, κ.λπ. κ.λπ. κ.λπ.

Ε λοιπόν ρωτήστε κι εμένα, και θα σας πω τη γνώμη μου. Αρχίζω.

Πιο καρακίτς δεκαετία δεν υπήρξε. Τα κορίτσια κυκλοφορούσαν με βάτες λες και ήταν η Τζόαν Κόλινς της Δυναστείας. Τα αγόρια είχαν "υπέροχα" μαλλιά λες και τραγουδούσαν στους Μίλι Βανίλι. Τα βιντεοκλάμπ ήταν φορτωμένα παραλλαγές του Ρόδα Τσάντα και Κοπάνα.

Ειτις. Μπούρδες.

Δεν συμφωνείτε, το ξέρω. Αλλά αυτό εννοώ.

Πάμε πιο πίσω. Προσθέστε άλλα 30-35 χρόνια, και αυτή η δεύτερη, αξιολογικώς φορτισμένη περιγραφή δίνει τη θέση της σε κάτι "τρίτο", το οποίον πλέον έχει ελάχιστη ή μηδενική σχέση με το πρώτο συμβάν. Συνοδεύεται όμως από πολλαπλάσια αξιολογική φόρτιση.

Η Κατοχή, ας πούμε. Όσοι την έζησαν, την έζησαν. Κάποιοι από αυτούς ζούνε ακόμα. Ό,τι θυμούνται, θυμούνται.

Όλοι μαζί όμως πιστεύουμε σήμερα πως ζούμε "σε κατοχή". Όπως στην κατοχή, σου λέει ο άλλος. Τσολάκηδες, γερμανοτσολιάδες, κομμουνιστοσυμμορίτες, σταλινικοί, εμφύλιος, κυβερνήσεις βουνού, ναζί, δεκεμβριανά, ο Σκόμπι, η Βάρκιζα, οι δωσίλογοι, η ΟΠΛΑ, οι εχθροί του έθνους, οι Νέοι Παρθενώνες, μπλα μπλα, μπλα μπλα μπλα.

Όλα αυτά βέβαια έχουν μικρή ως ελάχιστη σχέση με τα αρχικά συμβάντα. (Και πώς θα μπορούσε να είναι αλλιώς, άλλωστε;) Νομίζουμε πως αναφερόμαστε σε πράγματα που κάποιοι έστω τα θυμούνται αλλά στην ουσία αναφερόμαστε σε συνοπτικές περιγραφές των φίλτρων με τα οποία διαβάζουμε την πραγματικότητα. Ο ένας βλέπει παντού εχθρούς του έθνους. Ο άλλος βλέπει καπιταλιστές και γερμανοτσολιάδες.

Και μη νομίζετε πως πρόκειται για ελληνική εξαίρεση. Κοτζάμ Ευρώπη, κοτζάμ κόσμος, μια από τα ίδια. Σας το είχα πει, προ καιρού. Διαβάστε Τολστόι.

Και να' μαστε, παραμονές του 2016++ να φοράμε όλοι περιχαρείς τις καλύτερές μας παρωπίδες (και τα καλύτερά μας περιβραχιόνια), προετοιμαζόμενοι να επαναλάβουμε όλα εκείνα τα λάθη που ξέρουμε πια μια χαρά πώς να τα ξανακάνουμε. Ετσι, για το γούστο.

"Πρώτη φορά που μου ξανασυμβαίνει", που λέει και το ανέκδοτο.

Αλλά δεν πρόκειται για ανέκδοτο.

Καλή χρονιά, λοιπόν, αγαπητοί μου, αλλά μη τσιμπάτε. Δεν.

Σας ασπάζομαι,
Θείος Ακάκιος


CMYK & WEB
cmykandweb.gr
GRAPHIC DESIGN
design • layout • web

Skill: Beginner
Tags: openSUSE, YaST, encryption, LUKS, dm-crypt

Πρακτικές κρυπτογράφησης δεδομένων στο δίσκο

Για να επιζητείτε την ισχυρή κρυπτογράφηση των δεδομένων στους δίσκους δεν χρειάζεται να συνεργάζεστε με τον Snowden, ούτε να είστε μάχιμος αντιφρονών ενός καταπιεστικού καθεστώτος. Ευτυχώς, οι διαθέσιμες επιλογές για την υλοποίηση αξιόλογων μηχανισμών κρυπτογράφησης δεν είναι λίγες. Αν μάλιστα χρησιμοποιείτε Linux, τότε η παρεχόμενη ευελιξία είναι απεριόριστη και το οικονομικό κόστος μηδενικό.

Έχετε laptop, δικό σας ή δανεικό από την εταιρεία, το οποίο παίρνετε συχνά μαζί σας; Στον υπολογιστή στο σπίτι ή στο γραφείο, ποιοι άλλοι έχουν φυσική πρόσβαση; Σ' αυτές τις δύο και σε πάμπολλες άλλες περιπτώσεις, τι θα γίνει αν κάποιος μάθει το password του λογαριασμού σας ή απλά βγάλει και μεταφέρει αλλού το δίσκο του υπολογιστή; Ας θέσουμε το ερώτημα λίγο διαφορετικά: Αν πράγματι κάποιος αποκτήσει φυσική πρόσβαση στο δίσκο, πόσο θα ταραχτείτε σε μια κλίμακα από 1 έως 10; Μη βιαστείτε ν' απαντήσετε, τουλάχιστον όχι πριν θυμηθείτε τι έχετε αποθηκευμένο και ποιοι θα μπορούσαν να το εκμεταλλευτούν – ή έστω να θορυβηθούν αποκτώντας πρόσβαση σε πληροφορίες οι οποίες κανονικά είναι για τα μάτια σας και μόνο.

Βρήκατε τελικά πόσο θα ταραχτείτε, σ' αυτή την κλίμακα του 1 έως 10; Σ' όποιο νούμερο κι αν καταλήξατε, είμαστε βέβαιοι ότι βλέπετε τη θέση μας και κατανοείτε τον προβληματισμό μας. Ας μη γελιόμαστε. Η λύση για ηρεμία, γαλήνη και καθόλου άγχος –τουλάχιστον όσον αφορά στον έλεγχο της πρόσβασης σε ευαίσθητα δεδομένα–, είναι η ισχυρή κρυπτογράφηση επί του δίσκου. Εξετάζοντας αυτό το ενδεχόμενο, πολύ γρήγορα καταλήγουμε στην ακόλουθη λίστα προδιαγραφών:

- Η μέθοδος της κρυπτογράφησης οφείλει να 'ναι ισχυρή. Χωρίς το σχετικό password, η αποκρυπτογράφηση πρέπει να 'ναι πρακτικά αδύνατη.
- Οι μηχανισμοί κρυπτογράφησης οφείλουν να 'ναι "διάφανοι" για το χρήστη, υπό την έννοια ότι όλα πρέπει να γίνονται αυτόματα και, ει δυνατόν, χωρίς την παρουσία έξτρα λογισμικού.
- Ο υπολογιστικός φόρτος για τον επεξεργαστή δεν πρέπει να 'ναι μεγάλος – ή έστω να μη γίνεται αντιληπτός υπό καθημερινή, τυπική χρήση.

- Το όλο σύστημα της κρυπτογράφησης δεν πρέπει ν' αποτελεί black box. Αντίθετα, θέλουμε να 'ναι ανοικτό σε όσους ερευνητές επιθυμούν να ελέγξουν την αξιοπιστία του.

Linux to the rescue!

Μια λύση που ικανοποιεί τις τέσσερις προαναφερθείσες προδιαγραφές παρέχεται από κάθε σύγχρονη διανομή Linux. Αναφερόμαστε στο πρότυπο LUKS (Linux Unified Key Setup), για την κρυπτογράφηση αποθηκευτικών μέσων και τη διαχείριση των σχετικών κλειδιών, σε συνδυασμό με το υποσύστημα του πυρήνα ονόματι dm-crypt.

Το dm-crypt μπορεί κι αξιοποιεί οποιαδήποτε μέθοδο κρυπτογράφησης γνωρίζει ο πυρήνας, ενώ είναι κατάλληλο για κρυπτογράφηση δίσκων, κατατμήσεων ή file containers. Το πιο ενδιαφέρον χαρακτηριστικό του dm-crypt απορρέει από το γεγονός ότι ανήκει στο ευρύτερο υποσύστημα του πυρήνα ονόματι device mapper. Όταν κρυπτογραφούμε ένα αποθηκευτικό μέσο με τη βοήθεια του dm-crypt, ο πυρήνας ξαφνικά βλέπει ένα νέο block device ικανό να κρυπτογραφεί αυτόματα όλα τα δεδομένα που γράφουμε πάνω του. Φανταστείτε αν θέλετε ένα σκληρό δίσκο που ενσωματώνει hardware για την αυτόματη κρυπτογράφηση αλλά κι αποκρυπτογράφηση των δεδομένων (κι οφείλουμε φυσικά να γνωρίζουμε το κατάλληλο κλειδί αποκρυπτογράφησης). Κάπως έτσι αντιλαμβάνεται ο πυρήνας τα block devices που δημιουργεί το dm-crypt. Σε ένα τέτοιο device μπορούμε να έχουμε οποιοδήποτε σύστημα αρχείων θέλουμε (Ext4, XFS, ReizerFS κ.ά.), με μια άκρως ενδιαφέρουσα λεπτομέρεια: Τα ονόματα των αρχείων, τα δικαιώματα πρόσβασης και γενικότερα όλα τα metadata του εκάστοτε συστήματος αρχείων, είναι *επίσης* κρυπτογραφημένα. Σημειώστε εξάλλου ότι οι συσκευές που δημιουργεί το dm-crypt ενσωματώνονται πανεύκολα σε volume groups του LVM (Logical Volume Manager, https://deltahacker.gr/?p=1236). Εναλλακτικά, είναι δυνατόν ν' αποτελούν μέρη για τη δημιουργία τέτοιων groups.

Πρακτικά σενάρια χρήσης με το openSUSE

Αν τα προηγούμενα σάς είναι λίγο-πολύ άγνωστα και φαντάζουν κάπως αφηρημένα, δεν υπάρχει λόγος ανησυχίας. Το μόνο που χρειάζεται να έχετε κατά νου είναι ότι τα block devices που δημιουργεί το dm-crypt συμπεριφέρονται ως απλές κατατμήσεις ή δίσκοι. Όπως πιθανώς αντιλαμβάνεστε, ο συνδυασμός LUKS και dm-crypt προσφέρει μεγάλη ευελιξία αλλά κι ασφάλεια. Για άλλη μια φορά, ο καλύτερος τρόπος προκειμένου να συνειδητοποιήσουμε τι σημαίνει αυτό είναι με την εξέταση μερικών τυπικών σεναρίων χρήσης. Συγκεκριμένα, στο υπόλοιπο του παρόντος δουλεύουμε σε περιβάλλον openSUSE Leap και υλοποιούμε λύσεις για τις ακόλουθες τρεις περιπτώσεις:

α) κρυπτογραφημένο home partition κατά την εγκατάσταση του λειτουργικού

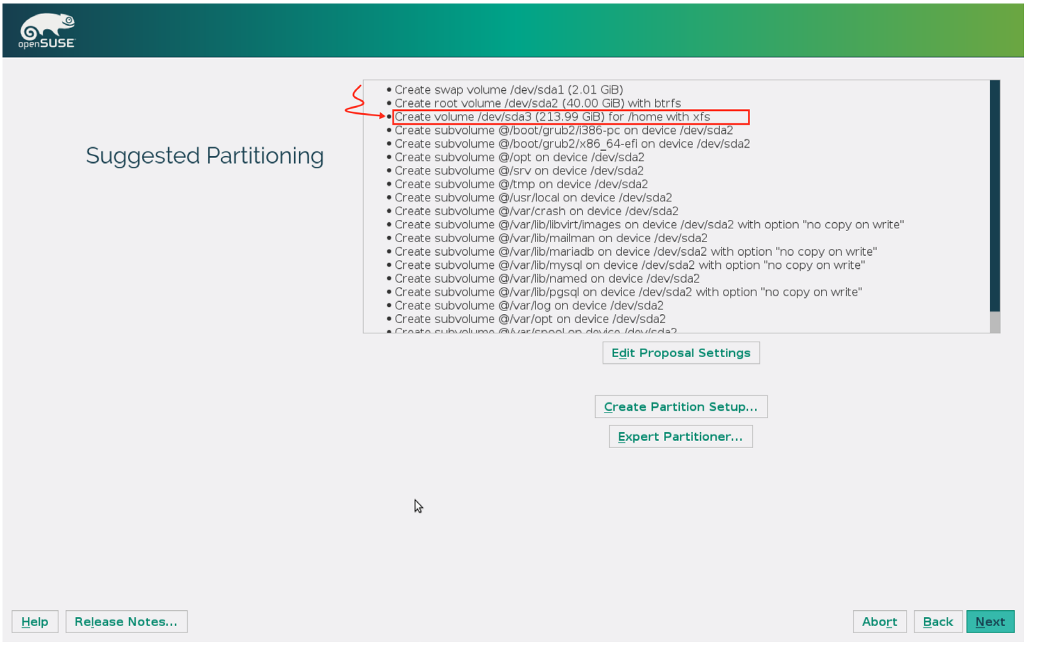
β) χρήση ξεχωριστού αρχείου ως encrypted file container

γ) αλλαγή μεγέθους κατάτμησης και δημιουργία νέας, κρυπτογραφημένης.

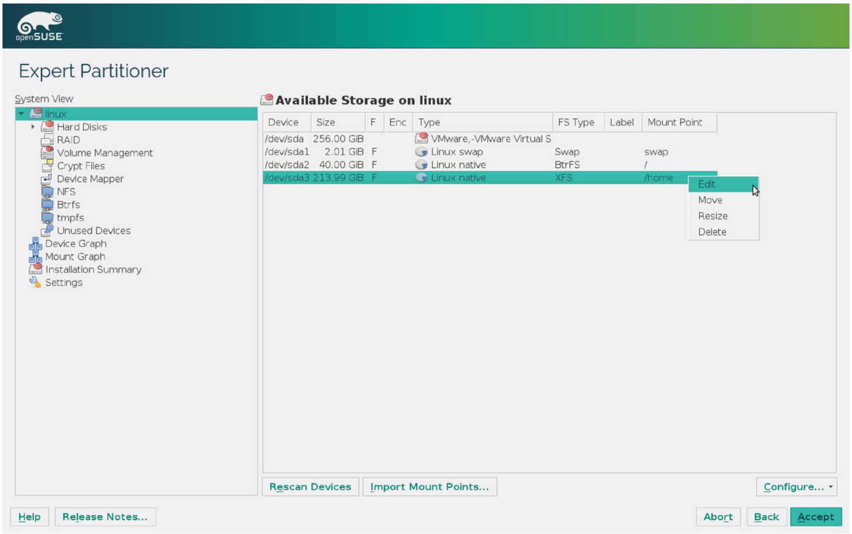
Χάρη στο πολυεργαλείο YaST του openSUSE, ακόμη και κάποιος με μηδενική εμπειρία στην κρυπτογράφηση μέσων αποθήκευσης είναι εύκολο να εφαρμόσει ένα οποιοδήποτε από τα τρία προηγούμενα σενάρια. Υπάρχουν βέβαια και κάποιες λεπτομέρειες, τις οποίες θα δούμε αναλυτικά στη συνέχεια.

Κρυπτογράφηση home partition κατά την εγκατάσταση

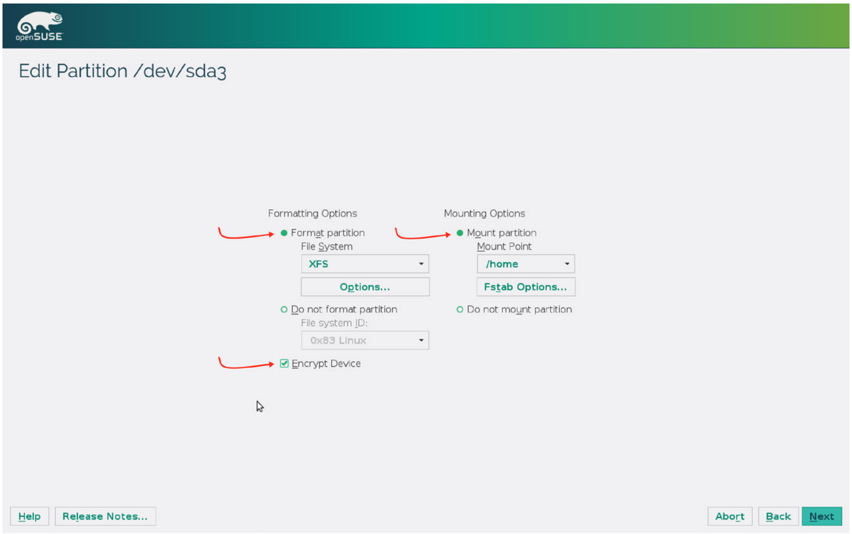
Ο ευκολότερος ίσως τρόπος προκειμένου να έχουμε μια κρυπτογραφημένη κατάτμηση στην οποία θα αποθηκεύονται όλα τα ευαίσθητα δεδομένα μας, είναι να τη δημιουργήσουμε μέσα από τον installer του openSUSE, στο στάδιο της εγκατάστασής του. Αξίζει, συγκεκριμένα, να φτιάξουμε μια ξεχωριστή κατάτμηση στην οποία θα προσαρτηθεί το /home, και να ζητήσουμε την κρυπτογράφησή της. Κατ' αυτόν τον τρόπο έχουμε *και* προστασία των δεδομένων αλλά *και* εύκολες αναβαθμίσεις του OS. Χάρη στο YaST του openSUSE, η διευθέτηση που συζητάμε επιτυγχάνεται με μερικά μόνο κλικ. Δείτε τα screenshots που ακολουθούν και διαβάστε τις αντίστοιχες περιγραφές.



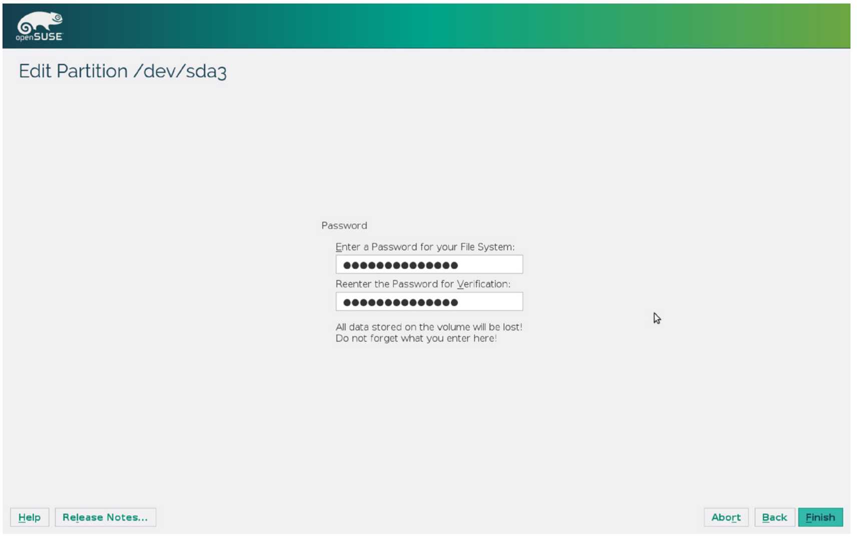
Η βασική πρόταση του YaST για τη διευθέτηση του δίσκου της εγκατάστασης αφορά σε ξεχωριστή κατάτμηση για το χώρο αντιμετάθεσης (swap partition), στη χρήση του νέου BtrFS για το root partition (μη σας μπερδεύουν τα subvolumes του BtrFS), καθώς και στη χρήση του "κλασικού" XFS για το /home. Στο παράδειγμά μας το swap partition έχει μέγεθος 2GB, το root partition έχει 40GB, ενώ τα υπόλοιπα 213GB αφιερώνονται στο partition για το /home. Επειδή επιπρόσθετα θέλουμε και την κρυπτογράφηση του προαναφερθέντος, απλά κάνουμε ένα κλικ στο κουμπί Expert Partitioner.



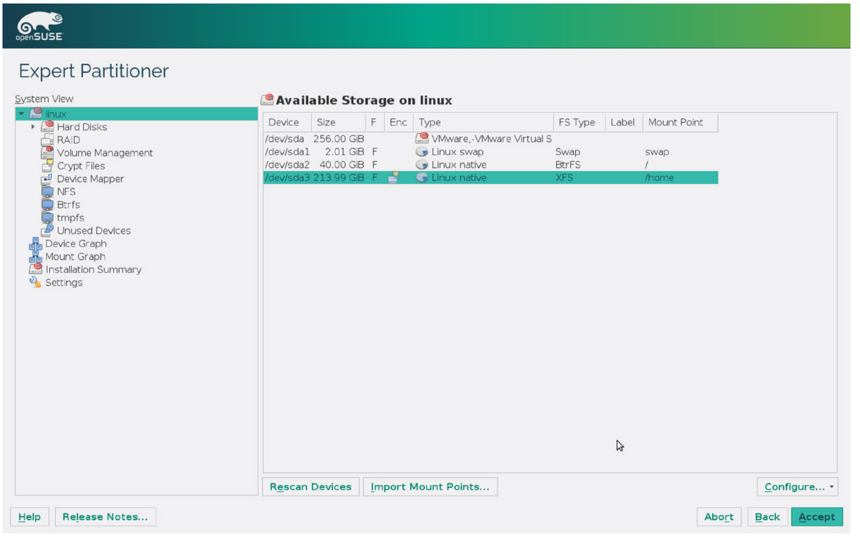
Ιδού μια πολύ πιο απλή κάτοψη της πρότασης του YaST για τις κατατμήσεις του δίσκου εγκατάστασης. Επιλέγουμε αυτή που μας ενδιαφέρει, δηλαδή αυτή που θα προσαρτηθεί στο /home, και με δεξί κλικ πάνω της διαλέγουμε το Edit.



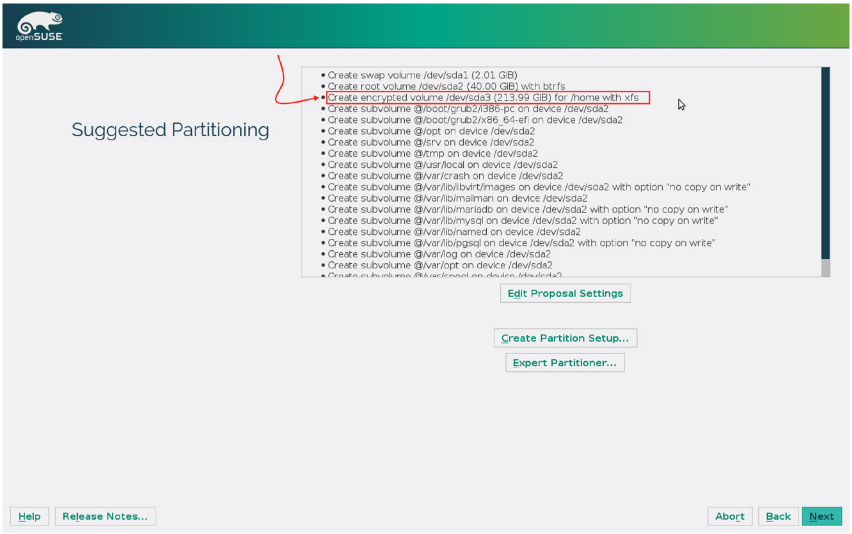
*Εδώ έχουμε την ευκαιρία να διαμορφώσουμε (format) την κατάτμηση, βεβαίως με το filesystem της επιλογής μας. Το προεπιλεγμένο είναι το XFS και είναι μια χαρά, ειδικά αν στην κατάτμηση πρόκειται ν' αποθηκεύονται μεγάλα αρχεία. Προσοχή, όμως: Αν κάποια στιγμή, μετά την εγκατάσταση του λειτουργικού, θελήσουμε να αλλάξουμε *μη καταστροφικά* το μέγεθος του διαμερίσματος, τότε αντί για το XFS οφείλουμε να στραφούμε στο Ext4. Ανεξαρτήτως του filesystem, δεν ξεχνάμε να τσεκάρουμε το κουτάκι Encrypt Device. Γι' αυτό άλλωστε ήρθαμε εδώ.*



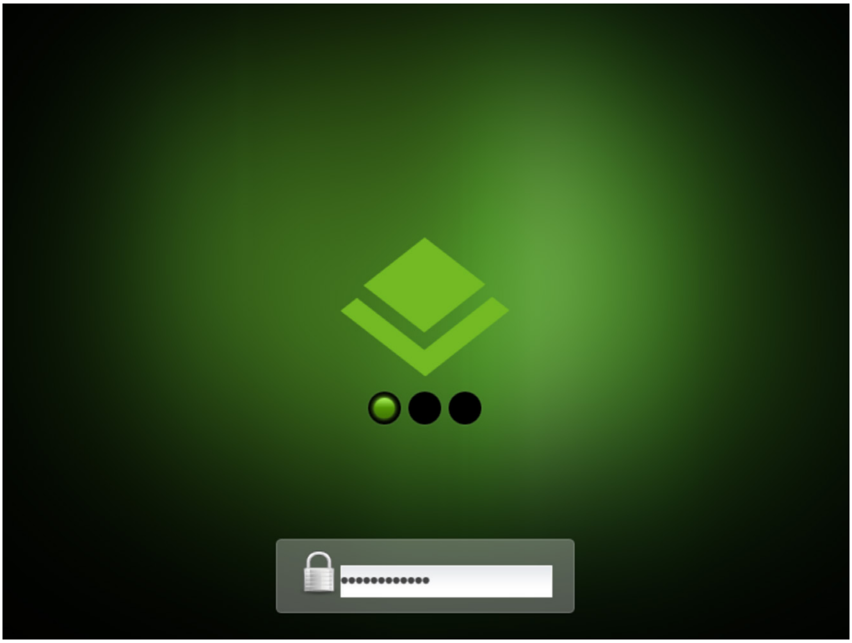
Αφού επιλέξαμε την κρυπτογράφηση του home partition, οφείλουμε τώρα να πληκτρολογήσουμε –δύο φορές, για λόγους ασφαλείας– ένα password. Κάθε φορά που ξεκινά το λειτουργικό, τη στιγμή που πρόκειται να προσαρτηθεί το home partition θα μας ζητείται το εν λόγω password. Είναι μάλλον περιττό να τονίσουμε ότι σε περίπτωση που το ξεχάσουμε δεν θα έχουμε κανέναν τρόπο και καμία ελπίδα για πρόσβαση στο /home.



Επιστροφή στη λίστα με τις κατατμήσεις. Πλέον, στην τομή της γραμμής του /home και της στήλης ονόματι Enc, υπάρχει ένα μικρό εικονίδιο που απεικονίζει έναν δίσκο μ' ένα λουκέτο πάνω του. Αυτό σημαίνει ότι η κατάτμηση πρόκειται να κρυπτογραφηθεί και προς τούτο απλά πατάμε στο Accept, κάτω δεξιά.



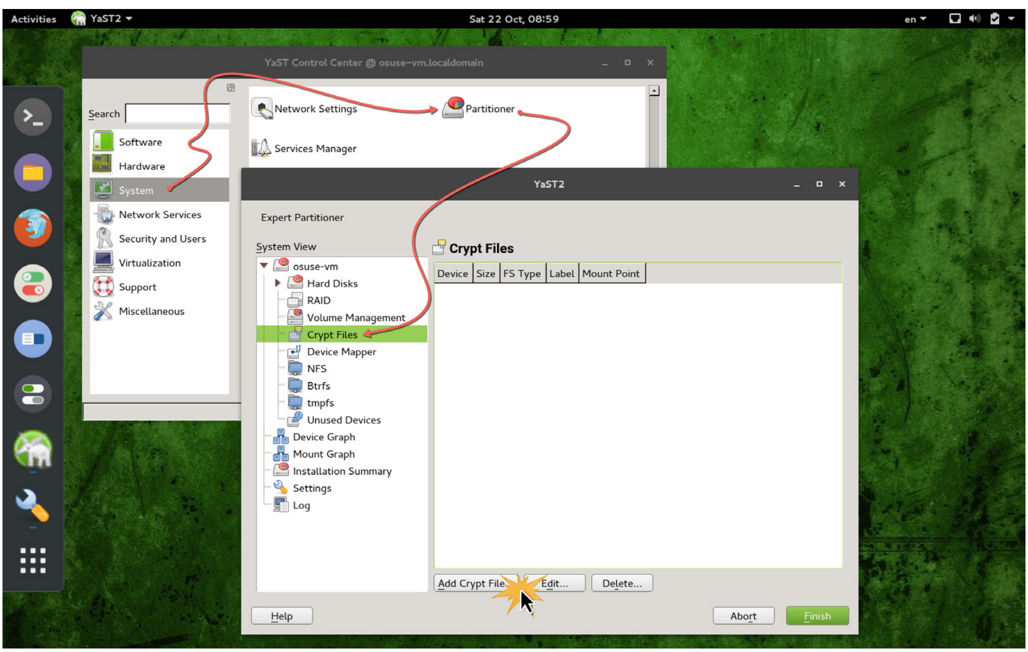
Παρατηρείτε τώρα κάποια διαφορά στην πρόταση του YaST; Ακριβώς!



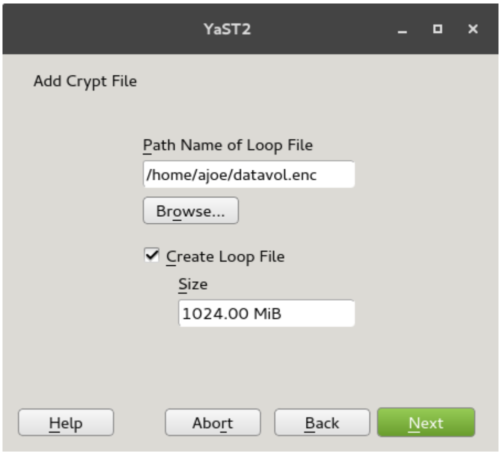
Μετά την εγκατάσταση του openSUSE και κάθε φορά που ανοίγουμε ή απανεκκινούμε τον υπολογιστή, η διαδικασία εκκίνησης θα σταματά κι εμείς θα πληκτρολογούμε το password για την αποκρυπτογράφηση του home partition.

Encrypted file containers

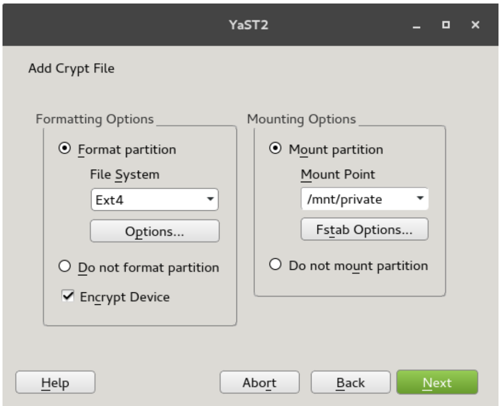
Αν το openSUSE Leap είναι ήδη στον υπολογιστή σας αλλά κατά τη διάρκεια της εγκατάσης δεν δώσατε σημασία στο ζήτημα της κρυπτογράφησης και τώρα έχετε δεύτερες σκέψεις (sic), πραγματικά δεν χρειάζεται να προβληματίζεστε. Αντί να ξεκινήσετε και πάλι τις εγκαταστάσεις, μια ιδέα είναι να δημιουργήσετε ένα αρχείο που θα συμπεριφέρεται ως κρυπτογραφημένος δισκάκος. Αναλυτικότερα, θα φτιάξετε ένα αρχείο συγκεκριμένου μεγέθους –όσο πιστεύετε ότι χρειάζεστε– και πάνω του θα δημιουργήσετε ένα filesystem. Θα έχετε έτσι ένα file container, το οποίο επιπρόσθετα θα κρυπτογραφήσετε. Μάλιστα η πρόσβαση στο περιεχόμενο του encrypted file container θα επιχειρείται αυτόματα κατά την εκκίνηση του λειτουργικού, αφού όμως πληκτρολογήσουμε το σχετικό password. Το encrypted file container μπορείτε να το φαντάζεστε ως ένα κρυπτογραφημένο USB stick το οποίο είναι μονίμως συνδεδεμένο στον υπολογιστή και σ' αυτό αποθηκεύετε αρχεία, όπως, π.χ., κλειδιά GnuPG/SSH/OpenVPN, έγγραφα με ευαίσθητες πληροφορίες κ.ο.κ. Προσέξτε τα screenshots που ακολουθούν και διαβάστε τις αντίστοιχες περιγραφές, ώστε να δείτε πώς φτιάχνουμε encrypted file containers με τη βοήθεια του YaST.



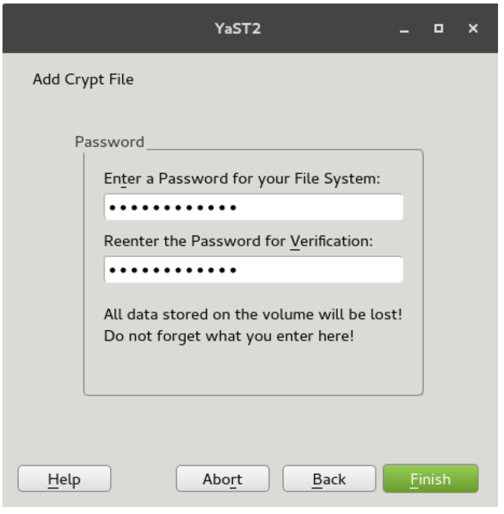
Ξεκινάμε το YaST κι από την κατηγορία System επιλέγουμε το module ονόματι Partitioner. Στο νέο παράθυρο που εμφανίζεται κάνουμε ένα κλικ στην κατηγορία Crypt Files. Θα φτιάξουμε τώρα το πρώτο μας encrypted file container. Ξεκινάμε με ένα κλικ στο κουμπί Add Crypt File.



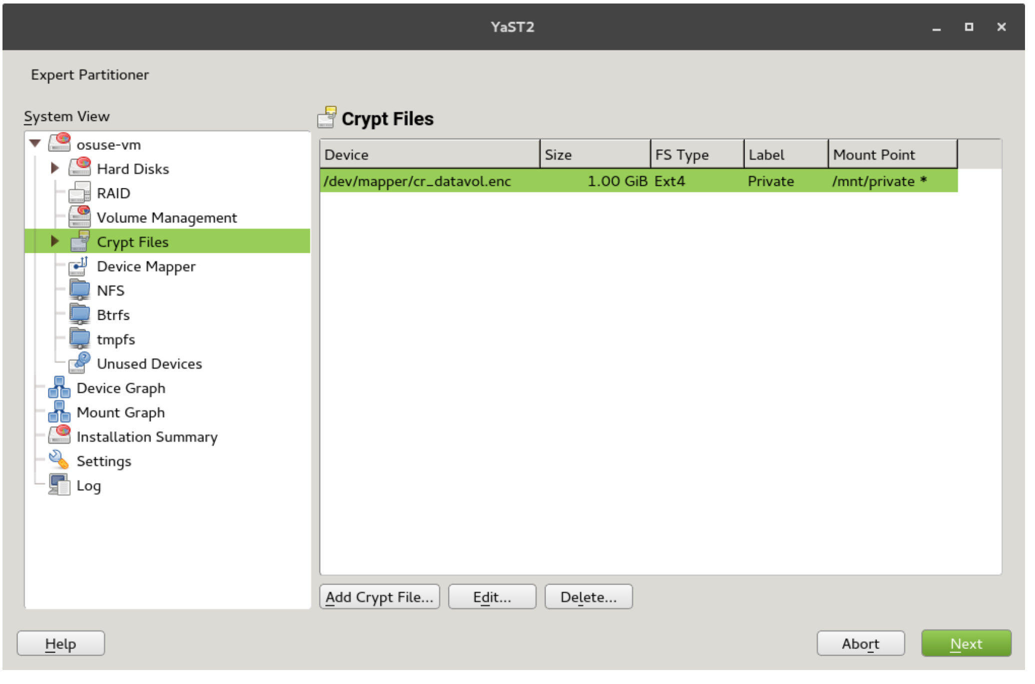
Στο Path Name of Loop File πληκτρολογούμε την πλήρη διαδρομή προς το αρχείο που θα αποτελέσει το encrypted file container. Αν το εν λόγω αρχείο δεν υπάρχει, το YaST θα το δημιουργήσει. Στο παράδειγμα, το αρχείο μας ονομάζεται datavol.enc και βρίσκεται εντός του προσωπικού καταλόγου του χρήστη με username το ajoe. Δεν ξεχνάμε να τσεκάρουμε το Create Loop File και στη θυρίδα από κάτω, με όνομα Size, πληκτρολογούμε το επιθυμητό μέγεθος του αρχείου. Όπως βλέπετε, φτιάξαμε ένα αρχείο μεγέθους 1GB. Αν ασχολείστε πρώτη φορά με τέτοια θέματα, επαναλαμβάνουμε ότι βοηθά να σκεφτόσαστε το loop file ως ένα USB stick το οποίο είναι μονίμως συνδεδεμένο στον υπολογιστή. Επιπρόσθετα, το συγκεκριμένο stick που τώρα ετοιμάζουμε θα έχει μια πολύ ενδιαφέρουσα ιδιότητα: ό,τι γράφουμε πάνω του θα κρυπτογραφείται αυτόματα. Αυτή την ιδιότητα της αυτόματης κρυπτογράφησης δεν την έχουμε ενεργοποιήσει ακόμη. Θα φροντίσουμε επ' αυτού σε πολύ λίγο, αφού πρώτα κάνουμε ένα κλικ στο κουμπί Next.



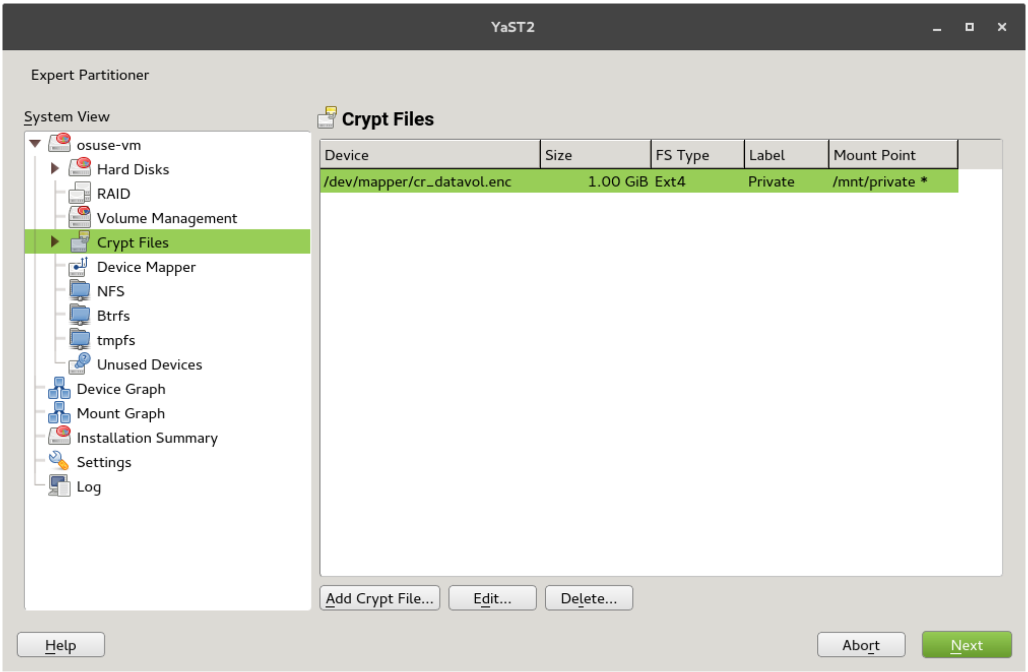
Επί του encrypted file container θα δημιουργήσουμε ένα filesystem, γι' αυτό κι επιλέγουμε το Format partition. Το σύστημα αρχείων Ext4 είναι ό,τι πρέπει –δοκιμασμένο, σταθερό αλλά και με πολύ καλές επιδόσεις σε τυπικά σενάρια χρήσης–, οπότε θέτουμε File System = Ext4. Θέλουμε βεβαίως και την κρυπτογράφηση του μέσου αποθήκευσης, συνεπώς τσεκάρουμε και το Encrypt Device. Η νέα κατάτμηση που θα δημιουργηθεί καλό είναι να προσαρτάται αυτόματα κατά την εκκίνηση του λειτουργικού, αλλά αφού πρώτα δώσουμε το password για το container file. Αυτό θα το ορίσουμε σε πολύ λίγο. Προς το παρόν διαλέγουμε το Mount partition και στη θυρίδα από κάτω, ονόματι Mount Point, πληκτρολογούμε την πλήρη διαδρομή του σημείου σύνδεσης ή αλλιώς προσάρτησης. Στο πλαίσιο του παραδείγματός μας, το σημείο σύνδεσης για την κατάτμηση είναι το /mnt/private. Με την προϋπόθεση ότι η κατάτμηση είναι επιτυχώς προσαρτημένη, ό,τι γράφουμε κάτω από το /mnt/private θα κρυπτογραφείται αυτόματα.



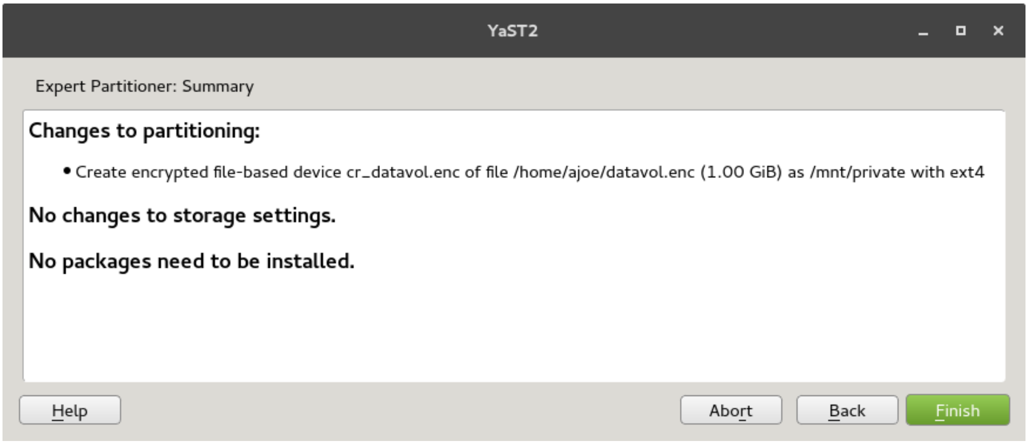
Για την προστασία του encrypted file container πληκτρολογούμε ένα password – δύο φορές, για λόγους ασφαλείας. Το password οφείλει να είναι ισχυρό, ώστε οι επιθέσεις brute force να είναι πρακτικά αδύνατες.



Ιδού μια σύνοψη των έως τώρα επιλογών μας. Παρατηρήστε το όνομα που έδωσε το YaST στο device file που αντιστοιχεί στην κατάτμηση του encrypted file container.



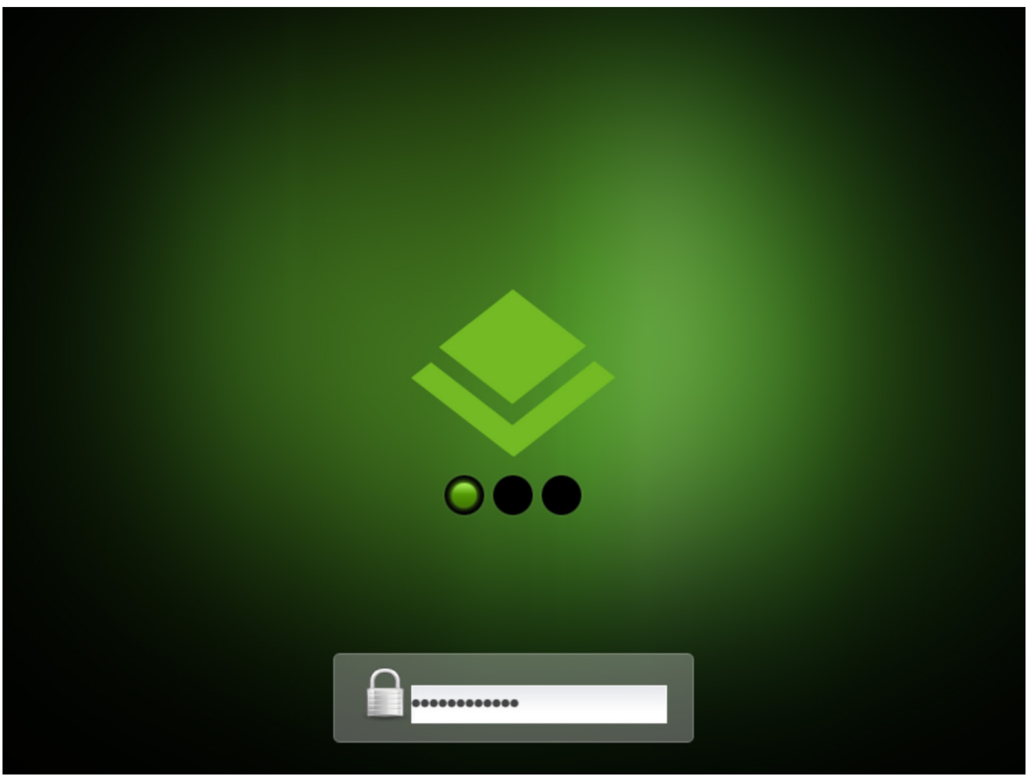
Περισσότερες λεπτομέρειες για τις εργασίες που πρόκειται να εκτελέσει το YaST. Ένα κλικ στο κουμπί Next είναι ό,τι χρειάζεται για την εκτέλεσή τους.



Προηγουμένως σας είπαμε ψέμματα: Χρειάζεται κι ένα κλικ, αυτή τη φορά στο κουμπί Finish.

```
ajoe@osuse-vm:~> df -hT
Filesystem                 Type      Size  Used Avail Use% Mounted on
devtmpfs                   devtmpfs  983M  8.0K  983M   1% /dev
tmpfs                      tmpfs     989M  532K  988M   1% /dev/shm
tmpfs                      tmpfs     989M  2.1M  987M   1% /run
tmpfs                      tmpfs     989M     0  989M   0% /sys/fs/cgroup
/dev/sda2                  ext4      9.8G  5.7G  3.7G  61% /
/dev/sdb1                  ext4     1008G   72M  957G   1% /mnt/storage-space
/dev/sda3                  xfs        52G  1.4G   51G   3% /home
/dev/mapper/cr_datavol.enc ext4      990M  1.3M  922M   1% /mnt/private
ajoe@osuse-vm:~>
```

Το YaST ολοκλήρωσε τις εργασίες που του υποδείξαμε και, όπως βλέπουμε κι από την έξοδο του df, η μία και μοναδική κατάτμηση του encrypted file container έχει προσαρτηθεί επιτυχώς κάτω από το /mnt/private.



Σε κάθε (επαν)εκκίνηση του συστήματος επιχειρείται αυτόματα πρόσβαση στο encrypted file container. Η διαδικασία πετυχαίνει μόνον αν πληκτρολογήσουμε το σωστό password και, στη συνέχεια, προσαρτάται και η κατάτμηση του container.

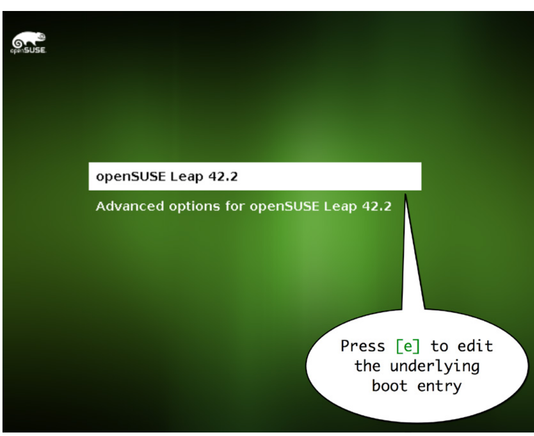
Εξασφάλιση ελεύθερου χώρου, δημιουργία κρυπτογραφημένου διαμερίσματος

Η λύση του encrypted file container είναι ό,τι πρέπει όταν τα δεδομένα που θέλουμε να προστατεύσουμε αποτελούνται από αρχεία το πολύ μεσαίου μεγέθους, ενώ αθροιστικά το μέγεθός τους δεν ξεπερνά τις μερικές δεκάδες gigabytes. Από εκεί και πάνω, καταλαβαίνετε ότι η διαχείριση του encrypted file container αρχίζει να γίνεται προβληματική. Σε τέτοιες περιπτώσεις, λοιπόν, είναι προτιμότερο να κρυπτογραφούμε έναν ολόκληρο φυσικό δίσκο – και το YaST καθιστά την όλη διαδικασία παιχνιδάκι. Όμως μερικές φορές δεν έχουμε ή απλά δεν θέλουμε να κρυπτογραφήσουμε έναν ολόκληρο δίσκο. Τότε, η αμέσως καλύτερη λύση είναι η κρυπτογράφηση μιας κατάτμησης – πάντα ενός φυσικού δίσκου. Για άλλη μια φορά το YaST θα αποδειχθεί πολύτιμο εργαλείο για τη δουλειά, αλλά σκεφτείτε και το πολύ πιθανό ενδεχόμενο ο δίσκος να *μη διαθέτει* τον απαιτούμενο ελεύθερο χώρο για τη δημιουργία νέας κατάτμησης. Τι κάνουμε, τότε; Τίποτε το ιδιαίτερο, απλά συνεχίζουμε να χρησιμοποιούμε το YaST. Το module για τη διαχείριση κατατμήσεων, βλέπετε, έχει μεταξύ άλλων τη δυνατότητα για μη καταστροφική συρρίκνωση υπαρχόντων κατατμήσεων, προκειμένου να δημιουργείται ελεύθερος χώρος για τη φιλοξενία μιας ή περισσοτέρων νέων κατατμήσεων. Συνοψίζοντας, στα screenshots που ακολουθούν βλέπουμε:

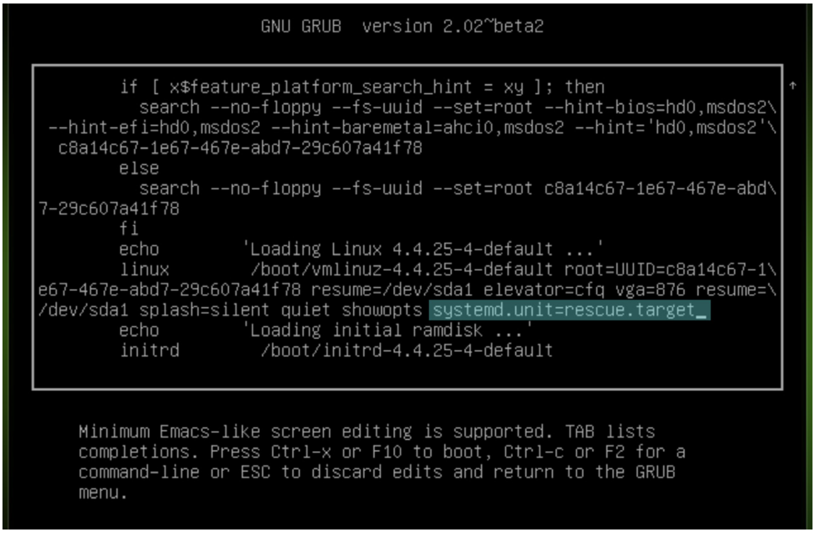
α) πώς ξεκινάμε τον υπολογιστή σε rescue mode, ώστε να έχουμε τη δυνατότητα για άνετη κι ασφαλή συρρίκνωση του home partition με τη βοήθεια του YaST

β) πώς φτιάχνουμε μια νέα κρυπτογραφημένη κατάτμηση στον ελεύθερο χώρο που δημιουργήθηκε, επίσης με τη βοήθεια του YaST.

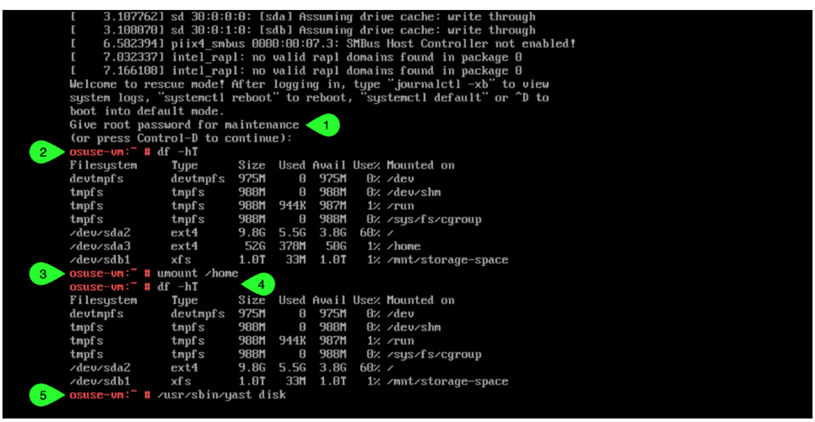
Σημειώστε εδώ ότι η μη-καταστροφική συρρίκνωση κατατμήσεων δεν είναι πάντα εφικτή. Ακριβέστερα, το αν είναι δυνατή ή όχι εξαρτάται από το filesystem της κατάτμησης. Αν, π.χ., το filesystem είναι το Ext4, τότε δεν έχουμε κανένα θέμα. Αν όμως η κατάτμηση είναι διαμορφωμένη με το XFS, τότε η συρρίκνωση –και γενικά η αλλαγή μεγέθους– της κατάτμησης χωρίς εκ νέου διαμόρφωση (format), είναι απλά αδύνατη. Ας παρακολουθήσουμε όμως μια εφαρμογή των προηγουμένων, μέσα από τα ακόλουθα screenshots και τις αντίστοιχες περιγραφές.



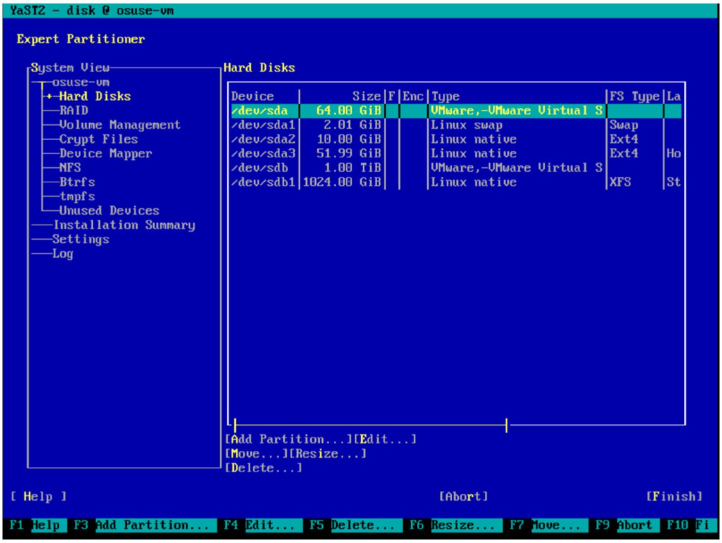
Θα αλλάξουμε το μέγεθος του home partition και γι' αυτό θα πρέπει πρώτα να το αποπροσαρτήσουμε. Καλό είναι λοιπόν να ξεκινήσουμε το λειτουργικό σε rescue mode, όπου κανείς άλλος χρήστης δεν θα 'ναι συνδεδεμένος, και να δουλέψουμε από το λογαριασμό του root. Επανεκκινούμε λοιπόν και μόλις εμφανιστεί το μενού του GRUB μετακινούμαστε πάνω από το entry που προκαλεί το φόρτωμα του openSUSE Leap. Αντί όμως να πατήσουμε το [Enter], πατάμε το πλήκτρο [e].



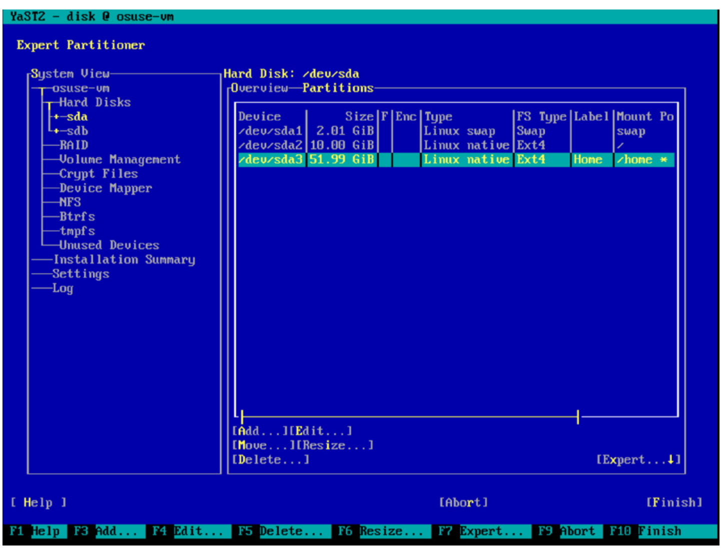
Έχουμε τώρα δυνατότητα για καθορισμό των παραμέτρων εκκίνησης του λειτουργικού. Στο τέλος της γραμμής που ξεκινά με "linux" (χωρίς εισαγωγικά) γράφουμε "systemd.unit=rescue.target" (επίσης χωρίς εισαγωγικά). Στη συνέχεια πατάμε το συνδυασμό πλήκτρων [CTRL+X] κι αμέσως ξεκινά το φόρτωμα του openSUSE Leap σε rescue mode. Παρεμπιπτόντως, αν δεν κατανοήσατε πλήρως τι είναι αυτό που μόλις κάναμε με το GRUB, αυτό ίσως οφείλεται στο γεγονός ότι δεν έχετε ακόμα διαβάσει το άρθρο μας περί του Systemd (https://deltahacker.gr/systemd-and-logging).



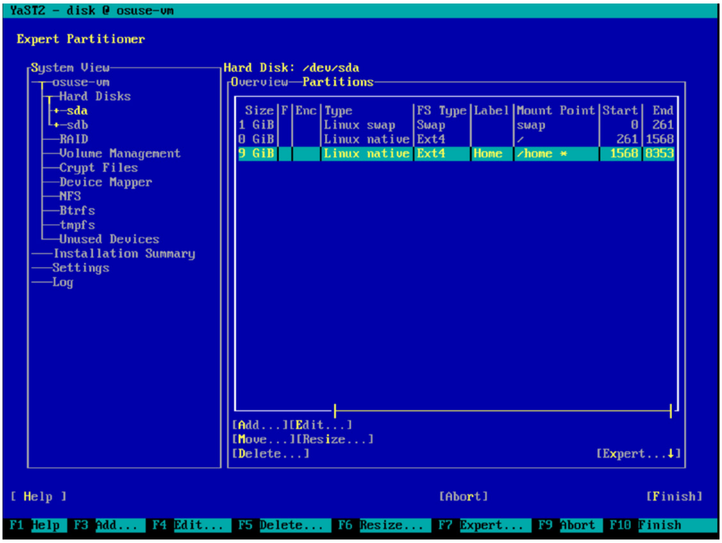
Λίγα δευτερόλεπτα αργότερα το openSUSE έχει φορτώσει σε rescue mode και φυσικά όχι σε περιβάλλον γραφικών. Συνδεόμαστε στο λογαριασμό του χρήστη root πληκτρολογώντας, απλά, το αντίστοιχο συνθηματικό. Στην έξοδο του εργαλείου df βλέπουμε ότι, αναμενόμενα, όλες οι κατατμήσεις είναι προσαρτημένες, βεβαίως κι εκείνη κάτω από το /home. Την αποσυνδέουμε κι αμέσως μετά τρέχουμε το YaST με την παράμετρο "disk" (χωρίς τα εισαγωγικά), ώστε να φορτώσει απευθείας το module για τη διαχείριση δίσκων και κατατμήσεων.



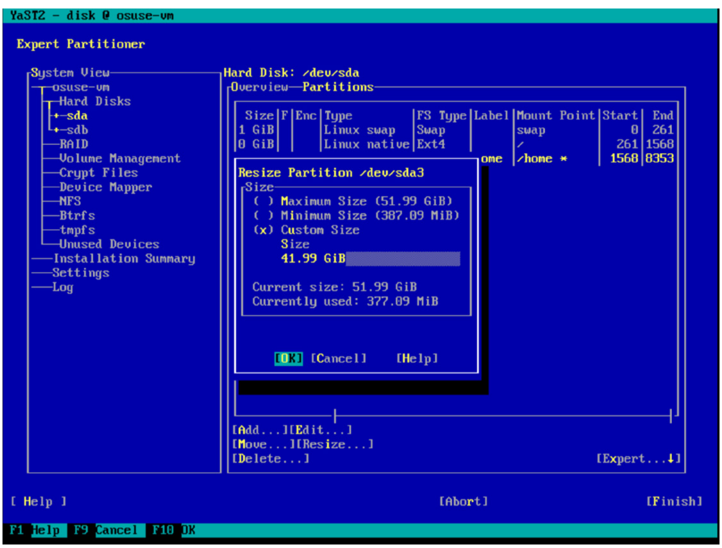
Βρισκόμαστε σε περιβάλλον κονσόλας κειμένου, οπότε το YaST σηκώνει το ανάλογο user interface. Όπως βλέπετε και στο παράδειγμά μας, φορτώνοντας το module ονόματι disk αρχικά παίρνουμε μια "κάτοψη" των δίσκων του υπολογιστή και των κατατμήσεών τους. Ο δίσκος που μας ενδιαφέρει είναι ο /dev/sda, αφού εκεί βρίσκεται το home partition.



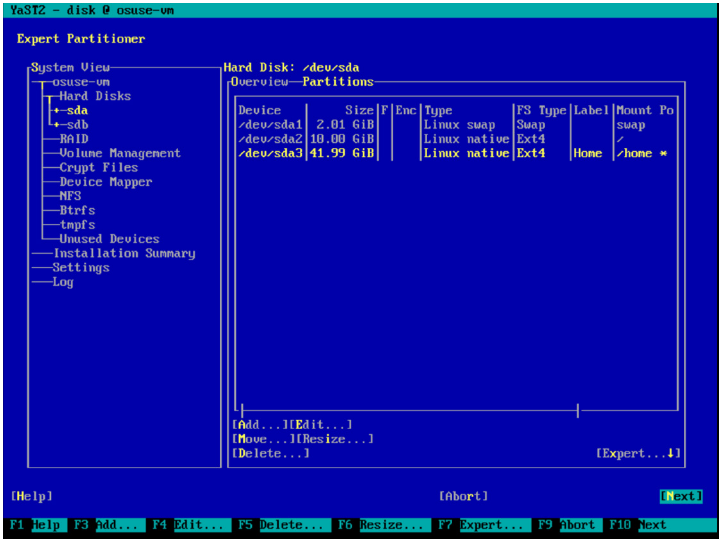
*Πατώντας διαδοχικά το πλήκτρο [Tab] φωτίζουμε (κυκλικά) διάφορα στοιχεία του user interface του YaST. Αφού μετακινηθούμε πάνω από τον δίσκο που μας ενδιαφέρει (/dev/sda, βλ. πλαίσιο Hard Disks) πατάμε το [Enter] κι έτσι βλέπουμε *μόνο* τις κατατμήσεις του συγκεκριμένου δίσκου. Είναι εξάλλου πιθανό τα περιεχόμενα του πλαισίου Hard Disks να μη χωρούν στην οθόνη. Ευτυχώς, μπορούμε να σκρολάρουμε προς τα δεξιά ή προς τ' αριστερά, πατώντας τα αντίστοιχα βελάκια του δρομέα.*



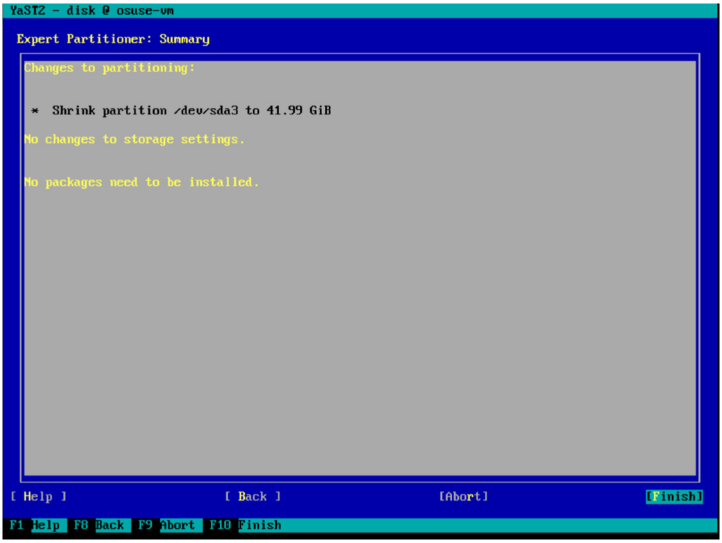
Σκρολάροντας λίγο προς τα δεξιά βεβαιωνόμαστε ότι το home partition είναι το /dev/sda3, έχει μέγεθος περίπου 52GB και το filesystem του είναι το Ext4.



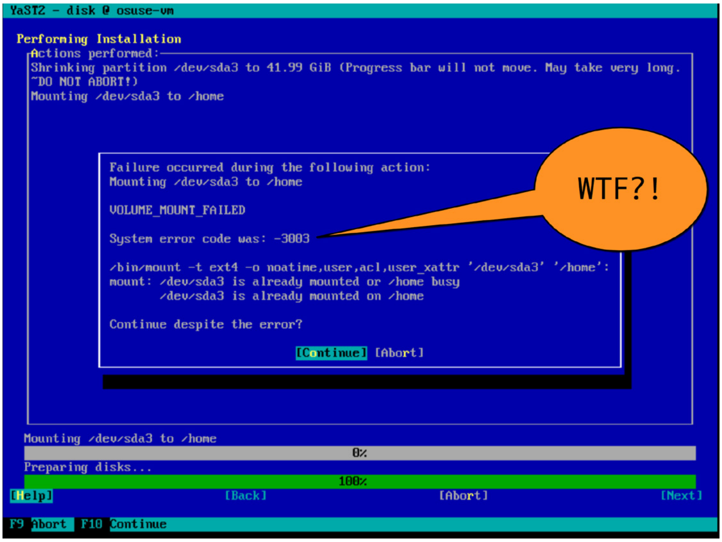
Για την αλλαγή μεγέθους μιας κατάτμησης φροντίζουμε ώστε να είναι φωτισμένη η γραμμή της (πατάμε μία ή περισσότερες φορές το πλήκτρο [Tab]) κι ακολούθως δίνουμε το συνδυασμό πλήκτρων [CTRL+I]. Γιατί αυτός ο συνδυασμός κι όχι κάποιος άλλος; Απλά προσέξτε τα κίτρινα γράμματα στις εντολές όπως Add, Edit, Move, Resize, Delete κ.ά. Στο pop-up που εμφανίζεται δίνουμε το νέο επιθυμητό μέγεθος της κατάτμησης. Όπως βλέπετε, στο παράδειγμα μειώνουμε το μέγεθος του home partition κατά 10GB: τόσα ακριβώς θα μας περισσεύουν για τη δημιουργία νέας, κρυπτογραφημένης κατάτμησης. Από τη στιγμή που είμαστε εντάξει με την αλλαγή μεγέθους της κατάτμησης, πατάμε το συνδυασμό πλήκτρων [ALT+O].



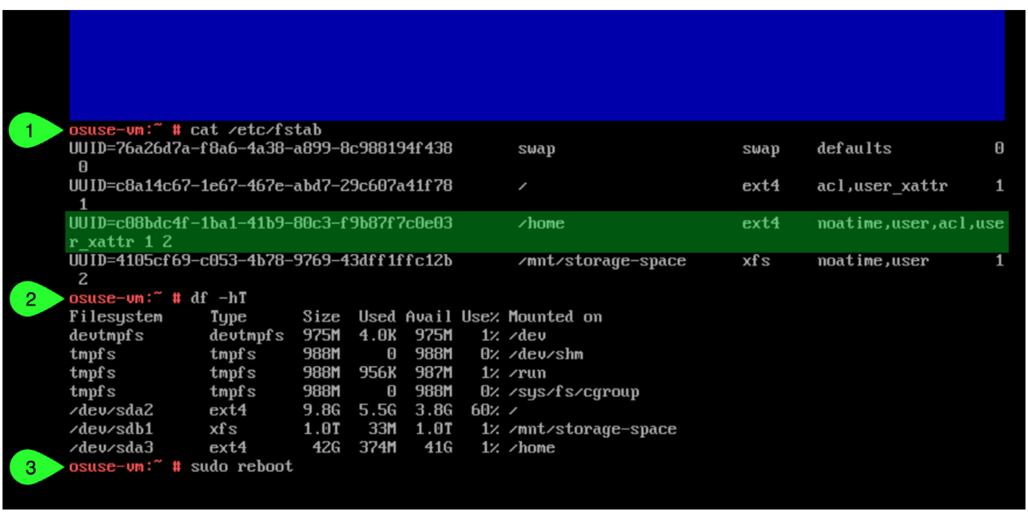
Ιδού η κατάτμηση του home, με το νέο μέγεθός της. Στην πραγματικότητα δεν έχει ακόμη αλλάξει κάτι. Για να γίνει κι αυτό, πατάμε το συνδυασμό πλήκτρων [ALT+N].



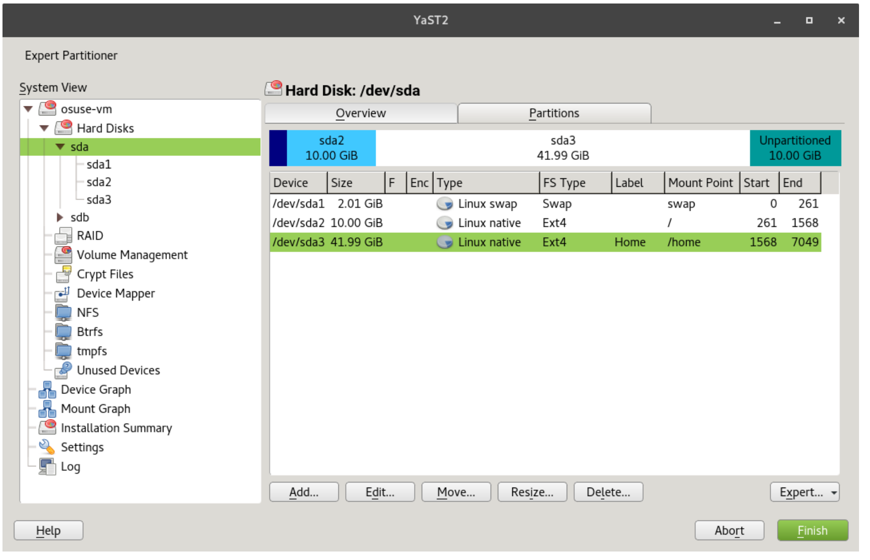
Πριν κάνει οτιδήποτε, το YaST μας ενημερώνει για το τι πρόκειται ν' ακολουθήσει. Στο παράδειγμά μας, το home partition θα μικρύνει κατά 10GB. Προσέξτε: Προς το παρόν δεν έχει γίνει καμία αλλαγή κι έχουμε δυνατότητα είτε να πάμε πίσω ώστε ν' αλλάξουμε κάτι ([ALT+B]), είτε ακόμη και ν' ακυρώσουμε την όλη επιχείρηση ([ALT+R]). Εφόσον είμαστε έτοιμοι και δεν θέλουμε κάποια αλλαγή, πατάμε το συνδυασμό πλήκτρων [ALT+F] ώστε να ξεκινήσει η διαδικασία μεταβολής μεγέθους – εν προκειμένω η διαδικασία της συρρίκνωσης.



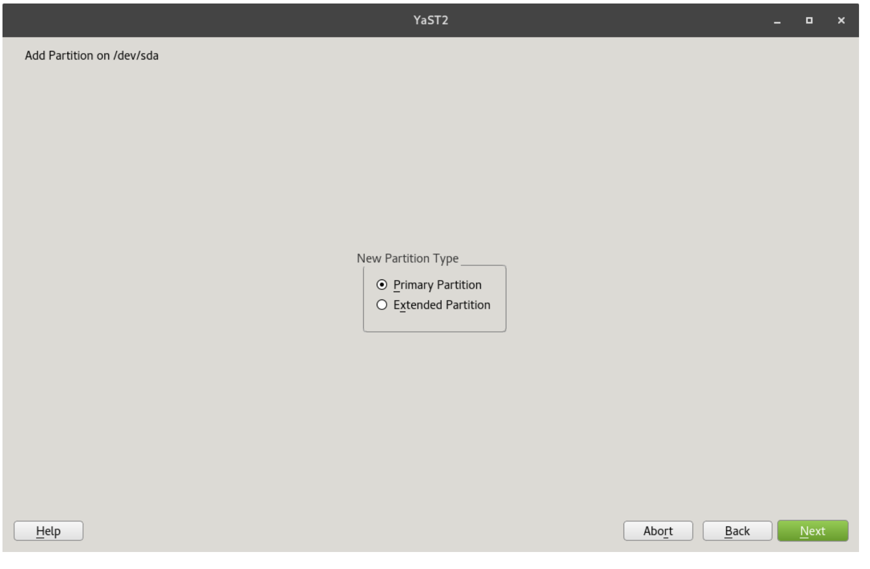
Μόλις ολοκληρωθεί η διαδικασία μεταβολής μεγέθους, το YaST είναι πιθανό να εμφανίσει ένα μήνυμα λάθους σαν το εικονιζόμενο (προσπαθεί να προσαρτήσει την κατάτμηση, ενώ είναι ήδη προσαρτημένη). Το συγκεκριμένο μήνυμα είναι εντελώς αθώο και μπορούμε να προχωρήσουμε πατώντας [ALT+O].



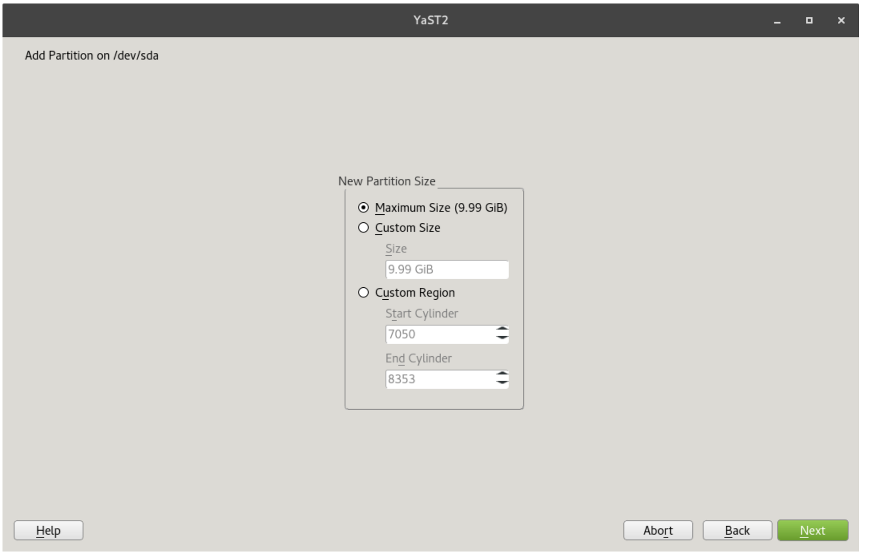
Ωραία, το YaST δεν έχει κάτι άλλο να κάνει, οπότε είμαστε και πάλι στη γραμμή εντολών. Με το df επαληθεύουμε ότι το home partition είναι προσαρτημένο, καθώς κι ότι το μέγεθος της κατάτμησης είναι μειωμένο κατά 10GB. Τόσος λοιπόν είναι ο διαθέσιμος χώρος για τη δημιουργία νέας κατάτμησης. Δεν υπάρχει λόγος να παραμείνουμε στην κονσόλα απλού κειμένου, οπότε επανεκκινούμε το λειτουργικό ώστε να συνεχίσουμε την εργασία μας από το περιβάλλον γραφικών.



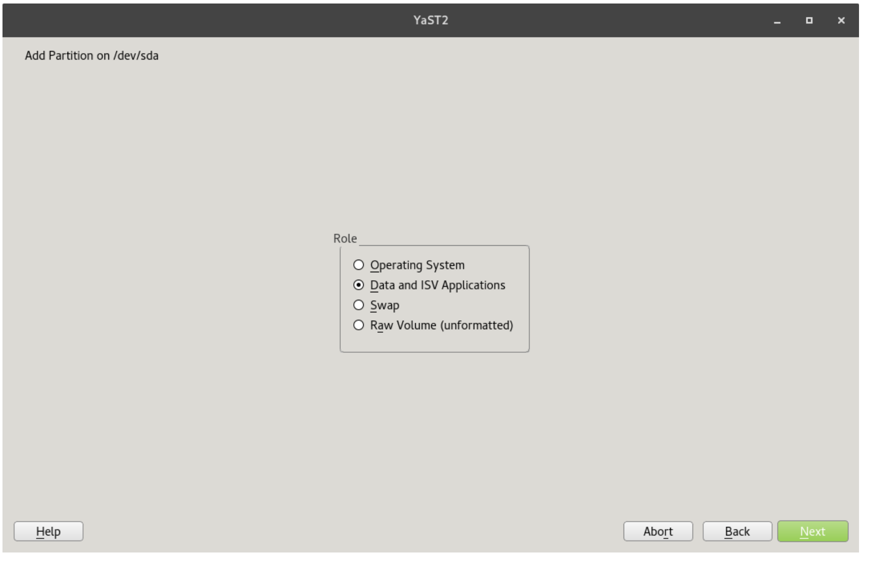
Βρισκόμαστε και πάλι στο περιβάλλον γραφικών και τώρα αντικρίζουμε τον Partitioner του YaST. Ο δίσκος /dev/sda είναι επιλεγμένος και, όπως βλέπετε, διαθέτει 10GB που δεν έχουν ακόμη κατανεμηθεί. Έχει, μ' άλλα λόγια, 10GB unpartitioned free space. Κάνουμε λοιπόν ένα κλικ στο κουμπάκι Add, ώστε εκεί να φτιάξουμε τη νέα κατάτμησή μας – η οποία θα είναι και κρυπτογραφημένη.



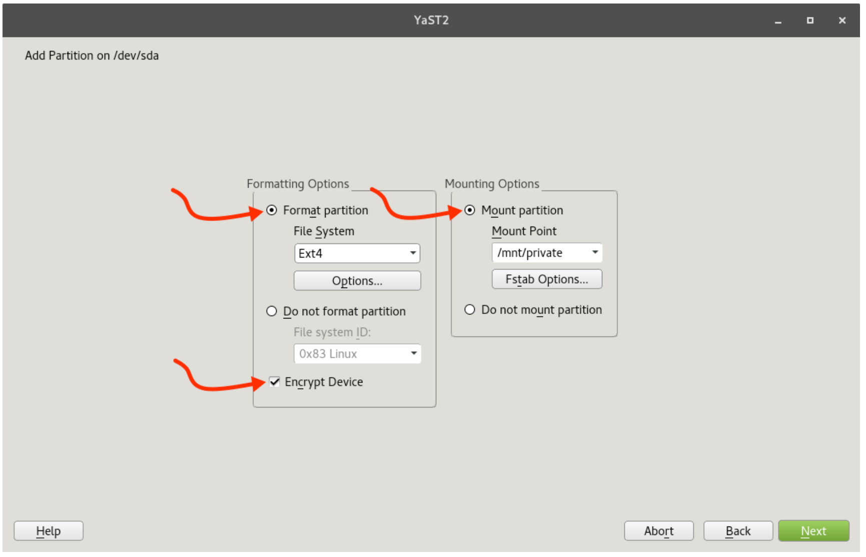
Η νέα κατάτμηση που φτιάχνουμε είναι τύπου Primary...



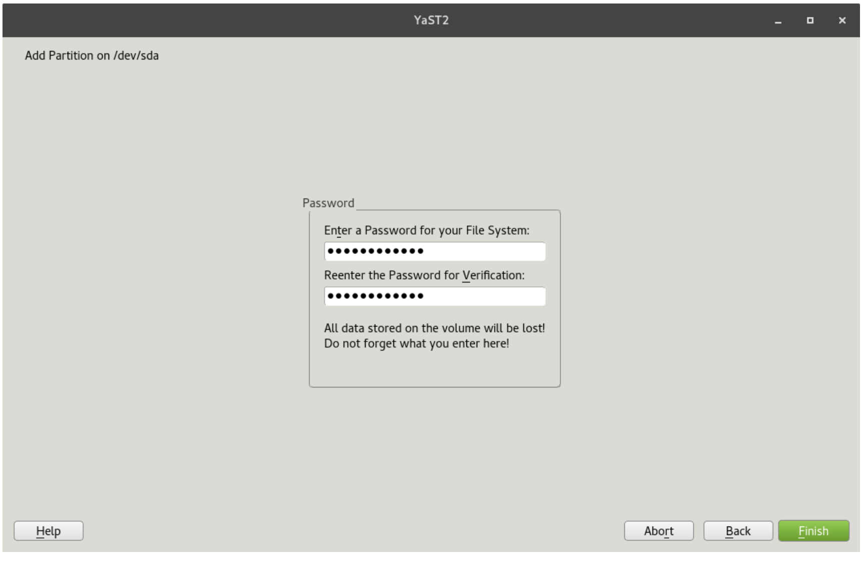
...κι επιθυμούμε να έχει τη μεγαλύτερη δυνατή χωρητικότητα.



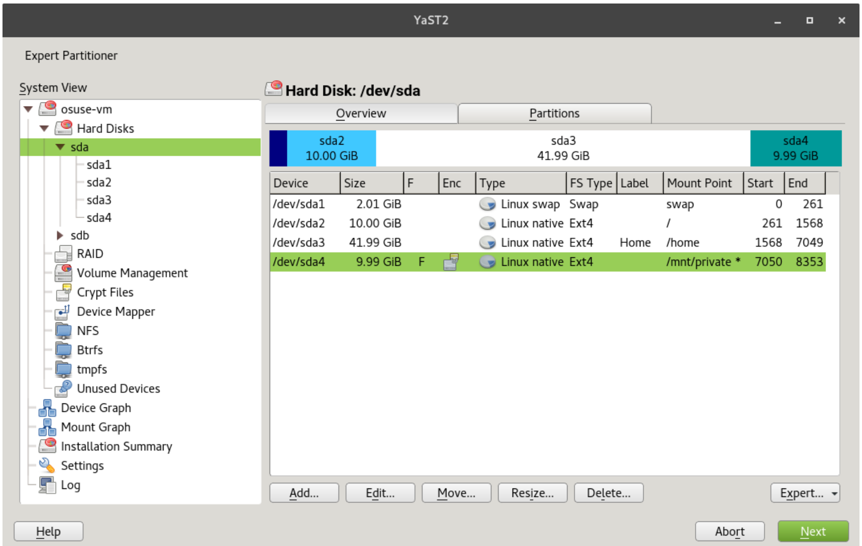
Ποιος θα 'ναι ο ρόλος της νέας κατάτμησης; Διαφορετικά: Για τι είδους χρήση την προορίζουμε; Δεν θα φιλοξενήσει λειτουργικό σύστημα (Operating System), δεν θ' αποτελέσει χώρο αντιμετάθεσης (Swap), δεν θα παραμείνει χωρίς filesystem (δεν θα 'ναι Raw Volume ή αλλιώς unformatted). Μας μένει, έτσι, ο ρόλος Data and ISV Applications (το ISV είναι αρκτικόλεξο του Independed Software Vendor), οπότε αυτόν επιλέγουμε.



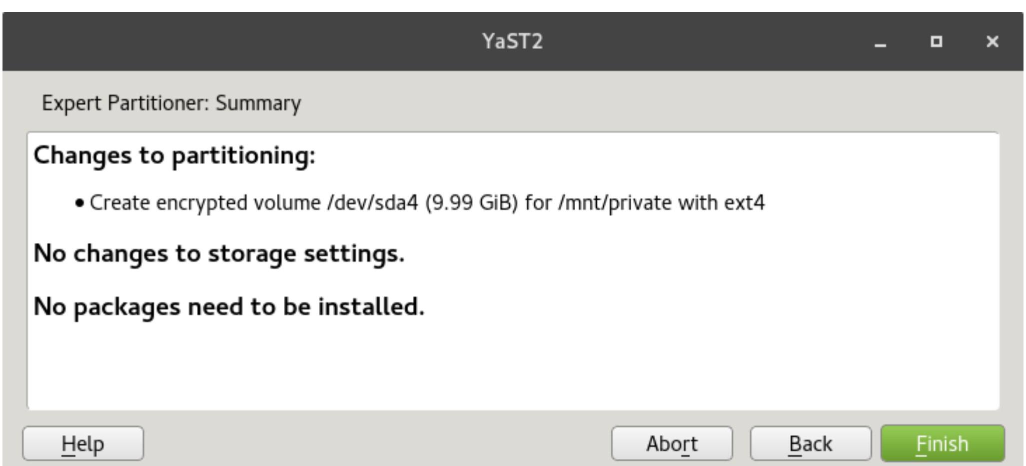
Με βάση το ρόλο που μόλις καθορίσαμε, το YaST προτείνει τώρα ένα filesystem για τη νέα κατάτμηση. Εμείς πάντως, ειδικά από τη στιγμή που πρόκειται να την κρυπτογραφήσουμε, επιλέγουμε το δοκιμασμένο Ext4. Τσεκάρουμε το κουτάκι Encrypt Device, ζητάμε την αυτόματη προσάρτηση της κατάτμησης, ενώ ως σημείο σύνδεσης ορίζουμε το /mnt/private.



Μόλις ζητήσαμε κρυπτογράφηση για την κατάτμηση, συνεπώς τώρα ορίζουμε το αντίστοιχο password (δύο φορές, για λόγους ασφαλείας).



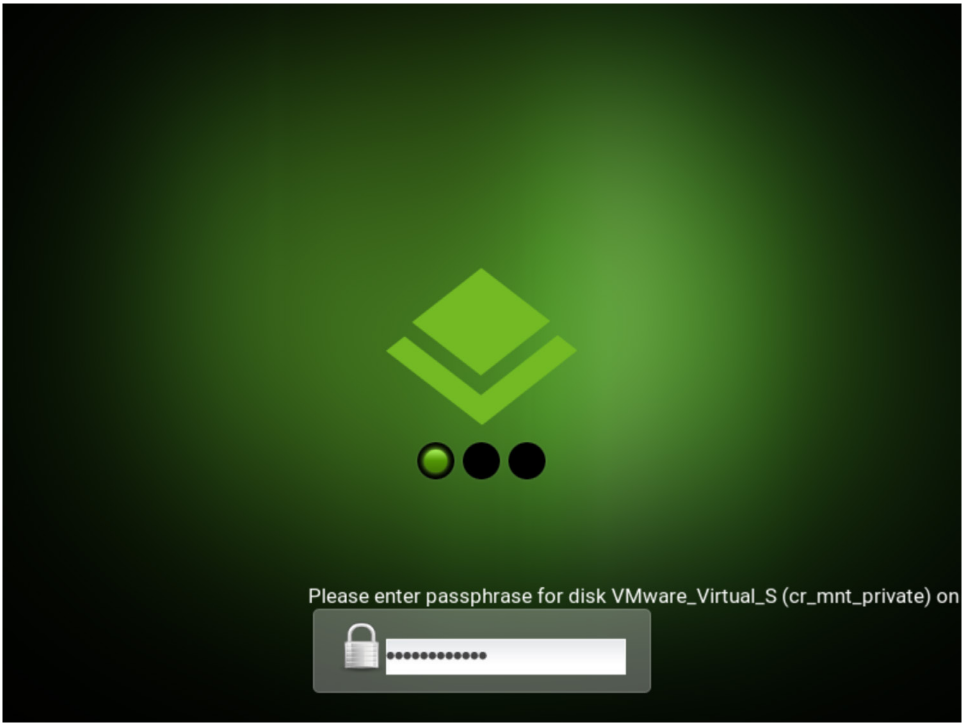
Τι πρόκειται να συμβεί σε πολύ λίγο; Η νέα πρωταρχική κατάτμηση (/dev/sda4) του δίσκου /dev/sda που έχει μέγεθος 10GB, πρόκειται να διαμορφωθεί κατά Ext4 (βλ. το "F") κι επίσης να κρυπτογραφηθεί (βλ. το εικονίδιο με το λουκετάκι πάνω από το δίσκο). Τέλος, θα προσαρτηθεί κάτω από το /mnt/private. Για όλα αυτά, ένα κλικ στο κουμπί Next είναι αρκετό.



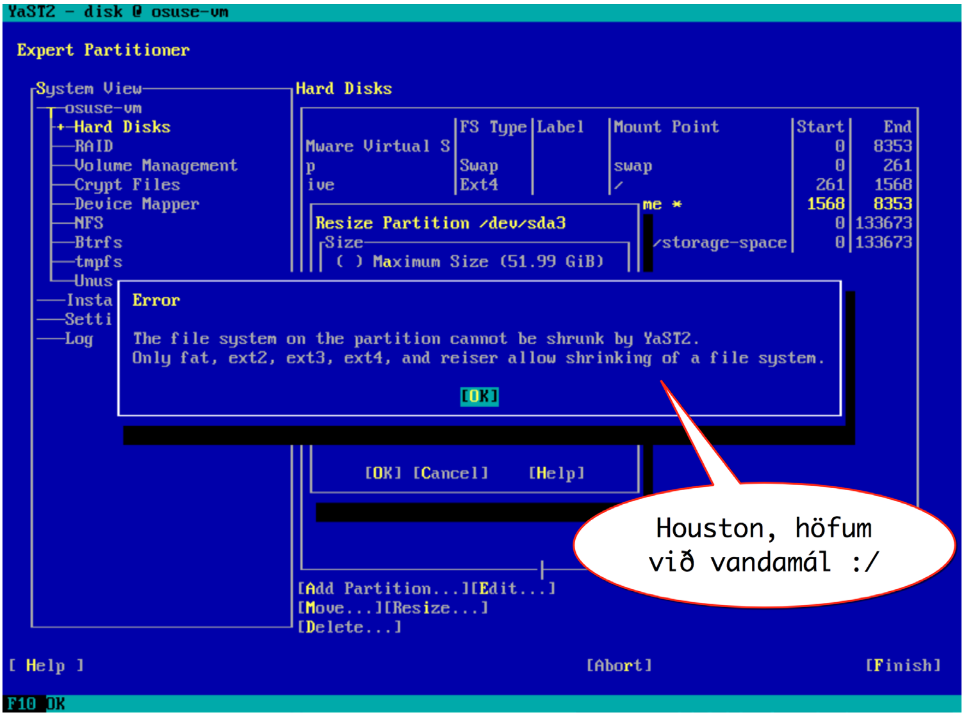
Τελευταία ευκαιρία ν' αλλάξουμε γνώμη! (Σιγά μην αλλάξουμε, αλλά λέμε τώρα.)

```
ajoe@osuse-vm:~>
ajoe@osuse-vm:~> cat /etc/fstab
UUID=76a26d7a-f8a6-4a38-a899-8c988194f438       swap                    swap    defaults                        0 0
UUID=c8a14c67-1e67-467e-abd7-29c607a41f78       /                       ext4    acl,user_xattr                  1 1
UUID=c08bdc4f-1ba1-41b9-80c3-f9b87f7c0e03       /home                   ext4    noatime,user,acl,user_xattr     1 2
UUID=4105cf69-c053-4b78-9769-43dff1ffc12b       /mnt/storage-space      xfs     noatime,user                    1 2
/dev/mapper/cr_mnt_private                      /mnt/private            ext4    noatime,acl,user_xattr,nofail   0 2
ajoe@osuse-vm:~>
ajoe@osuse-vm:~> df -hT
Filesystem                 Type      Size  Used Avail Use% Mounted on
devtmpfs                   devtmpfs  975M  4.0K  975M   1% /dev
tmpfs                      tmpfs     988M  200K  988M   1% /dev/shm
tmpfs                      tmpfs     988M  2.3M  986M   1% /run
tmpfs                      tmpfs     988M     0  988M   0% /sys/fs/cgroup
/dev/sda2                  ext4      9.8G  5.5G  3.8G  60% /
/dev/sdb1                  xfs       1.0T   33M  1.0T   1% /mnt/storage-space
/dev/sda3                  ext4       42G  374M   41G   1% /home
tmpfs                      tmpfs     198M   32K  198M   1% /run/user/1000
/dev/mapper/cr_mnt_private ext4      9.8G   23M  9.2G   1% /mnt/private
ajoe@osuse-vm:~>
```

Το YaST ολοκλήρωσε τις εργασίες του και η νέα μας, κρυπτογραφημένη κατάτμηση Ext4 είναι ήδη προσαρτημένη στο /mnt/private.



Έχουμε ζητήσει αυτόματη προσάρτηση της νέας κατάτμησης και, επειδή είναι κρυπτογραφημένη, κάθε φορά που (επαν)εκκινούμε τον υπολογιστή χρειάζεται να πληκτρολογούμε το αντίστοιχο password.



Bonus Screenshot. *Το YaST δεν είναι σε θέση να αλλάζει *μη-καταστροφικά* τα μεγέθη κατατμήσεων που είναι διαμορφωμένες με το XFS. Το ίδιο ισχύει και για άλλα εργαλεία, όπως, π.χ., είναι το GParded. Το αν μια κατάτμηση είναι δυνατόν να αλλάζει μέγεθος χωρίς να χάνει τα περιεχόμενά της, εξαρτάται από το filesystem που έχει. Στο screenshot φαίνονται τα συστήματα αρχείων που επιτρέπουν κάτι τέτοιο.*

Αντί επιλόγου

Τα δεδομένα που εμείς θέλουμε να έχουμε κρυπτογραφημένα δεν καταλαμβάνουν ιδιαίτερα πολύ χώρο. Συνήθως προστατεύουμε κλειδιά GnuPG, SSH και πιστοποιητικά OpenVPN, όπως επίσης κι έγγραφα διαφόρων τύπων. Για τις φωτογραφίες ή τα βίντεο δεν πολυνοιαζόμαστε, αφού εκεί δεν υπάρχει κάτι που θα σοκαριζόμασταν αν διέρρεε. Τώρα βέβαια που το σκεφτόμαστε λίγο καλύτερα, ίσως θα άξιζε να κρυπτογραφούμε *και* τις φωτογραφίες: ποτέ δεν ξέρεις τι μπορεί να κάνει ένας μέσος χρήστης του Photoshop! Πιθανώς το σκεπτικό σας να διαφέρει από το δικό μας και να θέλετε να κρυπτογραφείτε τα πάντα. Όπως και να 'χει, θέλουμε να πιστεύουμε ότι το παρόν άρθρο θα σας φανεί χρήσιμο. Δεν πρέπει τέλος να ξεχνάμε και το θέμα του backup. Αλλά αυτό είναι ένα άλλο θέμα, ίσως για κάποιο άλλο άρθρο.

Skill: Intermediate
Tags: openSUSE, YaST, SuSEfirewall2, iptables, OpenSSH, nmap, snapshots

Το δικό σας openSUSE, εκεί ψηλά!

Έχει γεμίσει το cloud με hosts που τρέχουν Ubuntu, φίλες και φίλοι. Σκοντάφτουμε επίσης διαρκώς και σε εγκαταστάσεις με Debian ή CentOS, αλλά το openSUSE πού είναι; Η διανομή Linux που δέχεται διαρκώς κι επιμελώς updates από τη στιβαρή, εταιρική εκδοχή server της SUSE, πού στο καλό κρύβεται στο cloud;

Επίμονα τα ερωτήματα κι αναζητούν εναγωνίως απάντηση. Προσφάτως είπαμε να σταματήσουμε ν' αναρωτιόμαστε κι αποφασίσαμε να ψάξουμε το θέμα λίγο καλύτερα. Γρήγορα υποψιαστήκαμε ότι αυτή η, φαινομενική τουλάχιστον, απουσία του openSUSE από το cloud, ίσως οφείλεται εν μέρει στο ότι VPS providers όπως η DigitalOcean (https://www.digitalocean.com) δεν το περιλαμβάνουν στις διαθέσιμες επιλογές για guest OS. Υπάρχουν όμως κι άλλοι μεγάλοι παίκτες του χώρου, όπως είναι η Linode (https://www.linode.com), οι οποίοι έχουν ήδη ξεκινήσει να προσφέρουν το openSUSE ως επιλογή. Εκτός από δημοφιλείς providers βρίσκουμε κι άλλους, λιγότερο γνωστούς αλλά σίγουρα αξιόλογους, οι οποίοι στα VPS και στους physical servers που ενοικιάζουν υποστηρίζουν *και* το openSUSE. Κατά νου έχουμε τη Γερμανική Hetzner Online (https://www.hetzner.de), μια εταιρεία με datacenters σε Νυρεμβέργη και Φρανκφούρτη στα οποία, παρεμπιπτόντως, χρησιμοποιούνται αποκλειστικά ανανεώσιμες πηγές ενέργειας.

Το openSUSE πάντως εξακολουθεί να *μην* είναι το OS που περιμένεις να τρέχει ένας server στο cloud. Ίσως το φαινόμενο να οφείλεται στο documentation – και συγκεκριμένα στην έλλειψη αυτού. Θα γνωρίζετε την κατάσταση με το Ubuntu: Όποιο θέμα κι αν σκεφτούμε, όποιο εγχείρημα κι αν ξεκινήσουμε, το πιθανότερο είναι ότι θα βρούμε να διαβάσουμε σχετικά guides και HOWTOs. Αν και σε μικρότερο βαθμό, το ίδιο ισχύει και για άλλες διανομές Linux όπως, π.χ., είναι το Debian, το Fedora ή το CentOS. Για το openSUSE, όμως; Χμ, για το openSUSE ισχύει το "Καλή τύχη". Ας μη γελιόμαστε: Το πλούσιο documentation για μια διανομή Linux όχι μόνο κρατάει τους υπάρχοντες χρήστες κοντά της, αλλά της φέρνει και νέους χρήστες. Φυσικά, ισχύει και το αντίστροφο.

Θα μπορούσαμε να παρομοιάσουμε τις διανομές Linux με πλανήτες και το documentation με την ατμόσφαιρα ενός πλανήτη. Φανταστείτε λοιπόν ότι έχετε την ευκαιρία να επισκεφτείτε έναν πλανήτη. Θα πηγαίνατε σε κάποιον με αραιή ή καθόλου ατμόσφαιρα ή σε κάποιον με πλούσια ατμόσφαιρα όπου μάλιστα μπορείτε άνετα ν' αναπνέετε, χωρίς ειδικό εξοπλισμό; Αν είσαστε ήδη σε έναν τέτοιο πλανήτη, πόσο εύκολα θα τον εγκαταλείπατε για κάποιον άλλον με φτωχότερη ατμόσφαιρα;

Ας πούμε ότι αισθάνεστε περιπετειώδεις κι αποφασίζετε να πάτε σε έναν πλανήτη με όχι-και-τόσο-καλή ατμόσφαιρα. Έτσι, για την εμπειρία. Με όλον τον απαραίτητο εξοπλισμό βάζετε μπρος και κάποια στιγμή φτάνετε σ' αυτόν τον άλλον πλανήτη, με την αραιή ατμόσφαιρα. Μάλιστα. Για πείτε μας τώρα, πόσο θα μείνετε εκεί;

Ο πλανήτης του openSUSE, φίλες και φίλοι, είναι πολύ όμορφος κι ενδιαφέρων και χωρίς ιδιαίτερη σεισμική ή ηφαιστειακή δραστηριότητα, θα μπορούσε όμως να 'χει καλύτερη ατμόσφαιρα. Το *γιατί* δεν έχει καλύτερη ατμόσφαιρα δεν θα μας απασχολήσει ιδιαίτερα. Είναι που δεν είμαστε κοσμολόγοι, ούτε καν γεωλόγοι. Και πριν αυτή η παρομοίωση πάψει να 'ναι χρήσιμη και γίνει απλά ενοχλητική, ας επιστρέψουμε στο προκείμενο. Και το προκείμενο είναι ότι το openSUSE δεν συναντάται τόσο συχνά στο cloud, εν πολλοίς διότι η ατμόσφαιρα –sorry, το διαθέσιμο documentation εννοούμε– άνετα θα μπορούσε να 'ναι πλουσιότερο.

Αντί να καθόμαστε και να θεωρητικολογούμε και να καταλήγουμε σε μάλλον αδιάφορες διαπιστώσεις, τι θα λέγατε να σηκώσουμε τα μανίκια και να πιάσουμε δουλειά; Εννοούμε βεβαίως να στρωθούμε και να γράψουμε documentation για το openSUSE. Όχι για να κατεβάσουμε άλλες διανομές από τα βάθρα τους στο cloud, αλλά γιατί ίσως πείσουμε μερικούς από εσάς να επιλέξετε το openSUSE για το επόμενο VPS σας. Αν το πετύχουμε θα χαρούμε, ενώ κι εσείς σίγουρα δεν θα το μετανιώσετε.

Το παρόν άρθρο είναι το πρώτο μιας νέας μίνι σειράς του deltaHacker. Στο πλαίσιό της θ' αναπτύξουμε θέματα που ενδιαφέρουν όσους έχουν –ή σκέφτονται ν' αποκτήσουν– VPS με openSUSE, επιθυμώντας να στήσουν το site τους ή γενικά κάποια web εφαρμογή. Αναλυτικότερα, στο πρώτο άρθρο ασχολούμαστε με τα ακόλουθα:

- αγορά VPS με openSUSE, από τη Hetzner Online
- πρώτη απομακρυσμένη σύνδεση και ρυθμίσεις
- ενίσχυση της ασφάλειας
- βασικές εργασίες διαχείρισης συστήματος
- λήψη snapshot (προαιρετικό)

Χωρίς άλλες περιστροφές, ας περάσουμε επιτέλους στο προκείμενο.

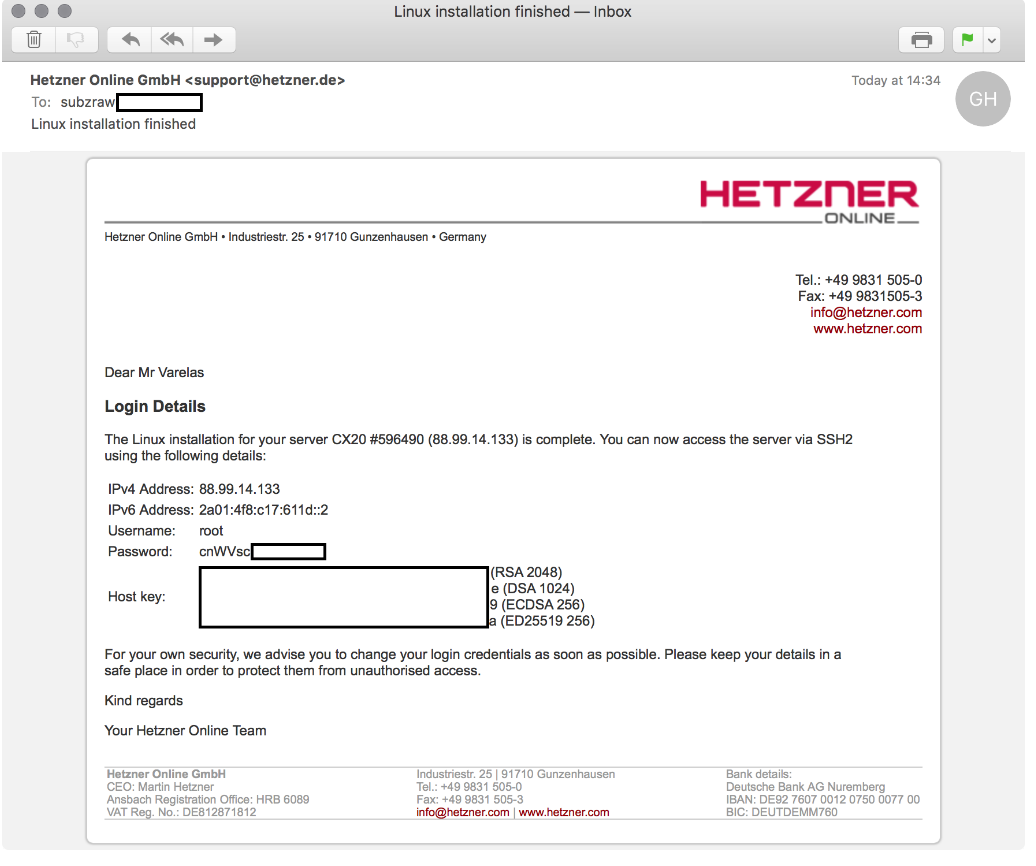
VPS με openSUSE από τη Hetzner

Δεν έχει νόημα να σας δείξουμε πώς ακριβώς αγοράζετε VPS από τη Hetzner (https://www.hetzner.de). Αξίζει όμως να σημειώσουμε ευθύς εξαρχής ότι θα εκπλαγείτε ευχάριστα με τις τιμές. Η εταιρεία ονομάζει τα VPS που προσφέρει vServers και διαθέτει έξι διαφορετικά μοντέλα: CX10, CX20, CX30, CX40, CX50 και CX60 (https://www.hetzner.de/gb/hosting/produktmatrix_vserver/vserver-produktmatrix). Το πιο φθηνό, το CX10, διαθέτει έναν εικονικό επεξεργαστή, 1GB RAM, δίσκο SSD στα 25GB, 2TB δωρεάν traffic κι ένα δωρεάν snapshot. Όλα αυτά με κόστος 3,90 ευρώ ανά μήνα χωρίς ΦΠΑ, επομένως 4,80 ευρώ/μήνα τελική τιμή. Δεν θέλουμε τώρα να κάνουμε συγκρίσεις με άλλους γνωστούς VPS providers, δείτε όμως το κόστος και τα χαρακτηριστικά ανάλογων VPS από άλλες εταιρείες. Μπορεί η διαφορά κόστους για τα εισαγωγικά VPS να 'ναι μικρή, διευρύνεται όμως αισθητά με τα μεγαλύτερα VPS. Εμείς, π.χ., αυτή τη στιγμή έχουμε δύο:

- ένα CX20 (2 cores, 2GB RAM, 50GB SSD, 5TB traffic, 2 δωρεάν snapshots) για 10,10 ευρώ/μήνα τελική τιμή
- ένα CX30 (2 cores, 4GB RAM, 100GB SSD, 8TB traffic, 3 δωρεάν snapshots) για 17,47 ευρώ/μήνα τελική τιμή

Στο CX30 έχουμε ήδη μεταφέρει δύο sites μας, ενώ πρόκειται να μεταφέρουμε και το deltahacker.gr. Το δε CX20 το χρησιμοποιούμε πειραματικά, κυρίως ως πλατφόρμα δοκιμών για άρθρα που ετοιμάζουμε για το περιοδικό – καλή ώρα όπως αυτό.

Σημείωση. Κατά την αγορά VPS από τη Hetzner Online υποδεικνύουμε το guest OS που θέλουμε να τρέχει. Οι επιλογές μας είναι Windows, Fedora, CentOS, Ubuntu, Debian και βεβαίως openSUSE Leap.



Linux installation finished — Inbox

Hetzner Online GmbH <support@hetzner.de>

To: subzraw[redacted]

Linux installation finished

Today at 14:34

GH

HETZNER ONLINE

Hetzner Online GmbH • Industriestr. 25 • 91710 Gunzenhausen • Germany

Tel.: +49 9831 505-0
Fax: +49 9831505-3
info@hetzner.com
www.hetzner.com

Dear Mr Varelas

Login Details

The Linux installation for your server CX20 #596490 (88.99.14.133) is complete. You can now access the server via SSH2 using the following details:

IPv4 Address: 88.99.14.133
IPv6 Address: 2a01:4f8:c17:611d::2
Username: root
Password: cnWVsc[redacted]
Host key: [redacted] (RSA 2048)
(DSA 1024)
(ECDSA 256)
(ED25519 256)

For your own security, we advise you to change your login credentials as soon as possible. Please keep your details in a safe place in order to protect them from unauthorised access.

Kind regards

Your Hetzner Online Team

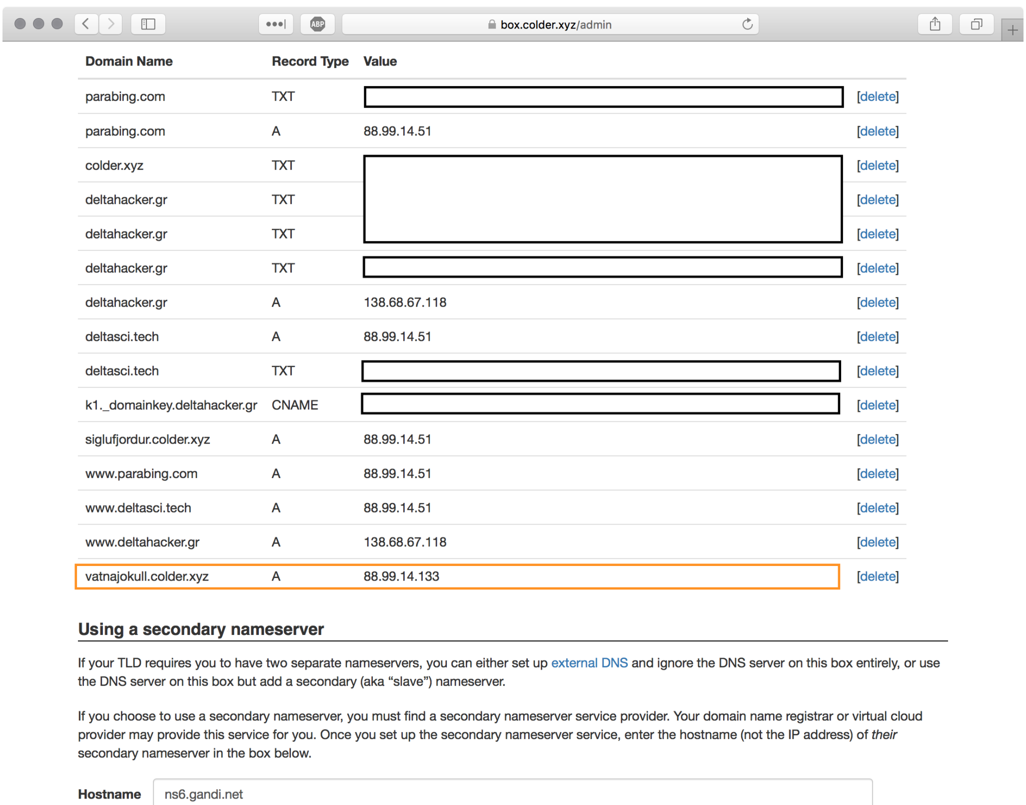
Hetzner Online GmbH
CEO: Martin Hetzner
Ansbach Registration Office: HRB 6089
VAT Reg. No.: DE812871812

Industriestr. 25 | 91710 Gunzenhausen
Tel.: +49 9831 505-0
Fax: +49 9831 505-3
info@hetzner.com | www.hetzner.com

Bank details:
Deutsche Bank AG Nuremberg
IBAN: DE92 7607 0012 0750 0077 00
BIC: DEUTDEMM760

Λίγα λεπτά μετά την αρχικοποίηση νέου VPS από τη Hetzner λαμβάνουμε σχετικό ενημερωτικό email. Στο μήνυμα αναφέρονται ο τύπος του VPS, το δημόσιο IP του και το προσωρινό συνθηματικό του χρήστη root. Εννοείται ότι, αφού συνδεθούμε μέσω SSH στον server, η πρώτη μας δουλειά θα είναι ν' αλλάξουμε το εν λόγω password. Εναλλακτικά, κατά τη δημι-

*ουργία VPS έχουμε τη δυνατότητα να υποδείξουμε το δημόσιο κλειδί SSH του τοπικού μας χρήστη, το οποίο θα προστεθεί στο αρχείο .ssh/authorized_keys του απομακρυσμένου root. Έτσι, από τον *συγκεκριμένο* τοπικό λογαριασμό θα συνδεόμαστε στον απομακρυσμένο λογαριασμό του root χωρίς πληκτρολόγηση password. Περισσότερα για τα passwordless SSH logins μπορείτε να διαβάσετε στο https://deltahacker.gr/?p=13357.*



Domain Name	Record Type	Value	
parabing.com	TXT		[delete]
parabing.com	A	88.99.14.51	[delete]
colder.xyz	TXT		[delete]
deltahacker.gr	TXT		[delete]
deltahacker.gr	TXT		[delete]
deltahacker.gr	TXT		[delete]
deltahacker.gr	A	138.68.67.118	[delete]
deltasci.tech	A	88.99.14.51	[delete]
deltasci.tech	TXT		[delete]
k1._domainkey.deltahacker.gr	CNAME		[delete]
siglufjordur.colder.xyz	A	88.99.14.51	[delete]
www.parabing.com	A	88.99.14.51	[delete]
www.deltasci.tech	A	88.99.14.51	[delete]
www.deltahacker.gr	A	138.68.67.118	[delete]
vatnajokull.colder.xyz	A	88.99.14.133	[delete]

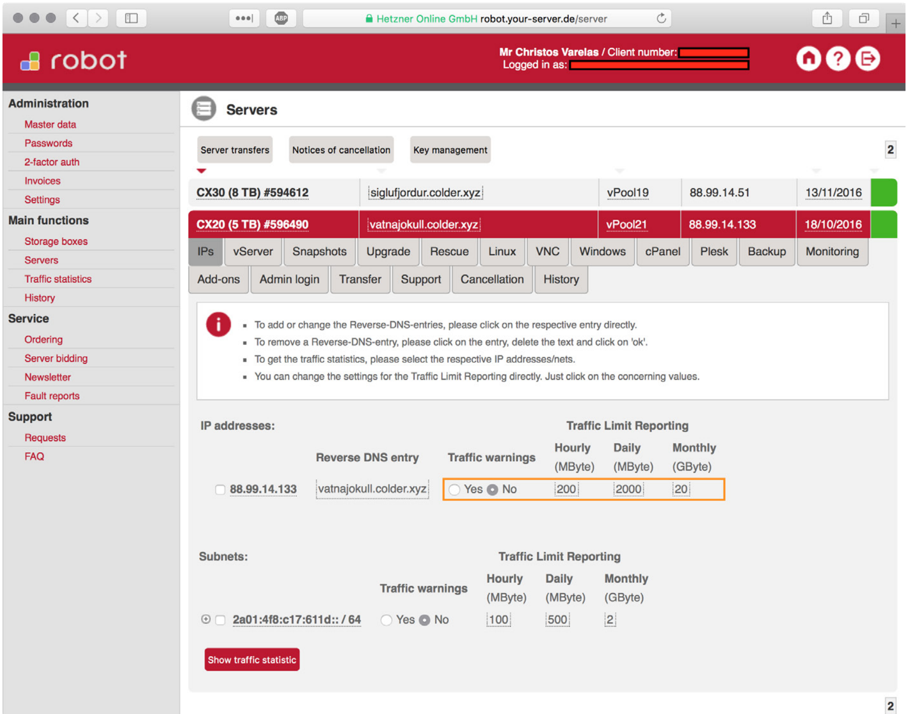
Using a secondary nameserver

If your TLD requires you to have two separate nameservers, you can either set up external DNS and ignore the DNS server on this box entirely, or use the DNS server on this box but add a secondary (aka "slave") nameserver.

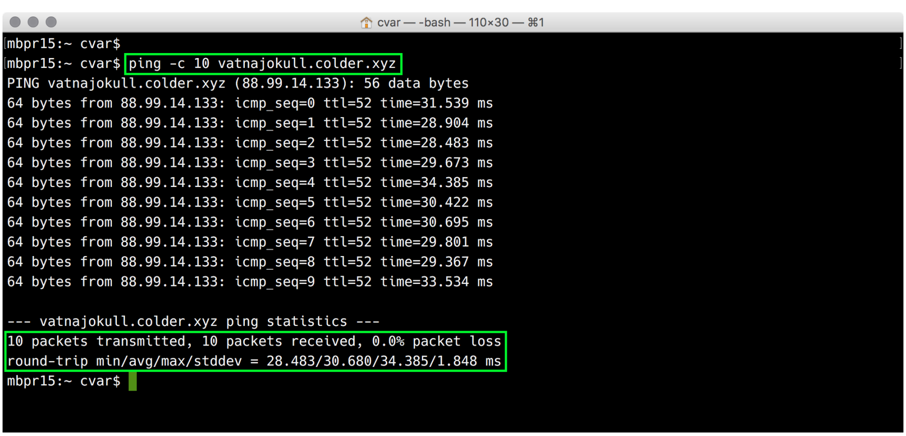
If you choose to use a secondary nameserver, you must find a secondary nameserver service provider. Your domain name registrar or virtual cloud provider may provide this service for you. Once you set up the secondary nameserver service, enter the hostname (not the IP address) of *their* secondary nameserver in the box below.

Hostname ns6.gandi.net

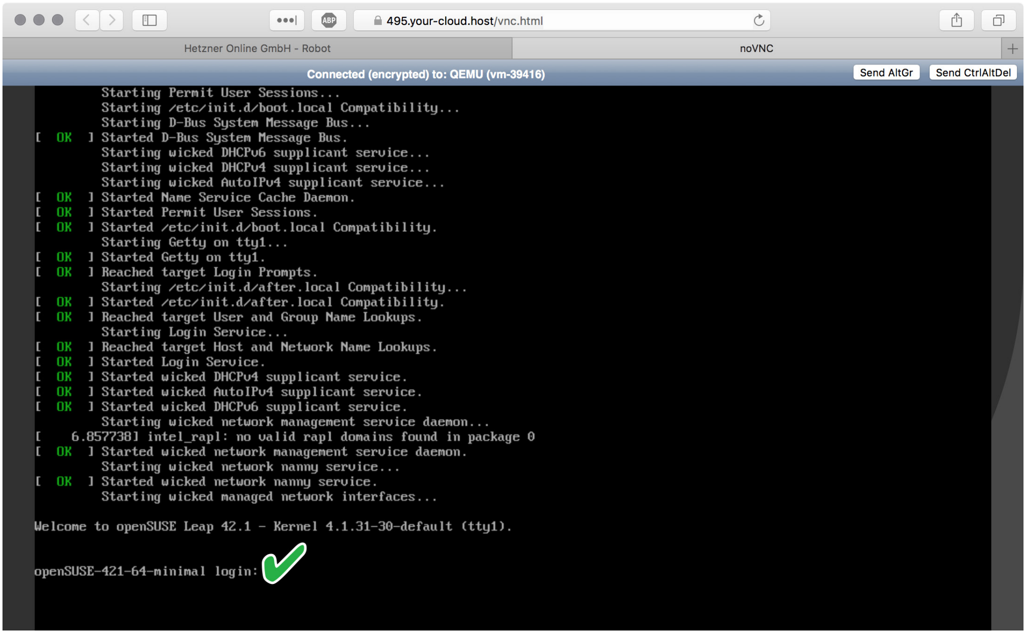
Προαιρετικά, αν διαθέτουμε κάποιο domain τότε μπορούμε να αντιστοιχίσουμε το ίδιο ή κάποιο subdomain του στο νέο VPS. Στο παράδειγμα, από το web panel του nameserver που συνοδεύει τον προσωπικό μας mailserver (https://deltahacker.gr/?p=14096), στο νέο VPS έχουμε αντιστοιχίσει το subdomain με όνομα vatnajokull.colder.xyz. Έτσι, αντί για το IP του VPS αρκεί να πληκτρολογούμε το πολύ πιο απλό vatnajokull.colder.xyz :P



Μια όψη του web panel της Hetzner, όπου φαίνονται τα δύο VPS μας. Θα παρατηρήσετε ότι το web panel δεν είναι ό,τι πιο εύχρηστο ή "διαισθητικό" υπάρχει Εκεί Έξω (ΤΜ). Προσφέρει μολαταύτα ένα πλούσιο σύνολο λειτουργιών στον ενδιαφερόμενο χρήστη. Δείτε, π.χ., ότι παρέχεται δυνατότητα για αυτόματες ειδοποιήσεις μέσω email, κάθε φορά που ξεπερνιούνται συγκεκριμένα όρια στη διακίνηση των πακέτων.



Ένας γρήγορος έλεγχος για το (α) αν το DNS resolving δουλεύει, (β) το VPS μας είναι προσβάσιμο από το Internet.



Από το web panel της Hetzner παρέχεται κονσόλα VNC για καθένα από τα VPS μας. Στο screenshot φαίνεται ξεκάθαρα ότι το λειτουργικό του VPS (openSUSE Leap) έχει φορτώσει επιτυχώς. Αν θέλουμε συνδεόμαστε στο λογαριασμό του root μέσω της κονσόλας, πληκτρολογώντας το αντίστοιχο συνθηματικό. Είναι όμως πολύ πιο βολικό να συνδεόμαστε μέσω SSH από τον αγαπημένο μας client ή απλά από τη γραμμή εντολών ενός τερματικού. Εμείς αυτό ακριβώς κάνουμε, οπότε αυτό και σας προτείνουμε.

Πρώτη σύνδεση, hostname και domain name

Κατά την πρώτη μας σύνδεση στο VPS μέσω SSH κάνουμε login στο λογαριασμό του root. Αν κατά τη δημιουργία του VPS *δεν* υποδείξατε το δημόσιο κλειδί του τοπικού σας χρήστη –εμείς, π.χ., δεν το υποδείξαμε–, τώρα θα χρειαστεί να πληκτρολογήσετε το προσωρινό password του απομακρυσμένου χρήστη root. Αυτό το βρίσκουμε στο email που στέλνει η Hetzner αμέσως μετά την αρχικοποίηση του VPS. Πρώτο μας μέλημα είναι η αλλαγή του προσωρινού password, χρησιμοποιώντας το εργαλείο passwd:

```
openSUSE-421-64-minimal:~ # passwd
New password:
Retype new password:
passwd: password updated successfully
openSUSE-421-64-minimal:~ #
```

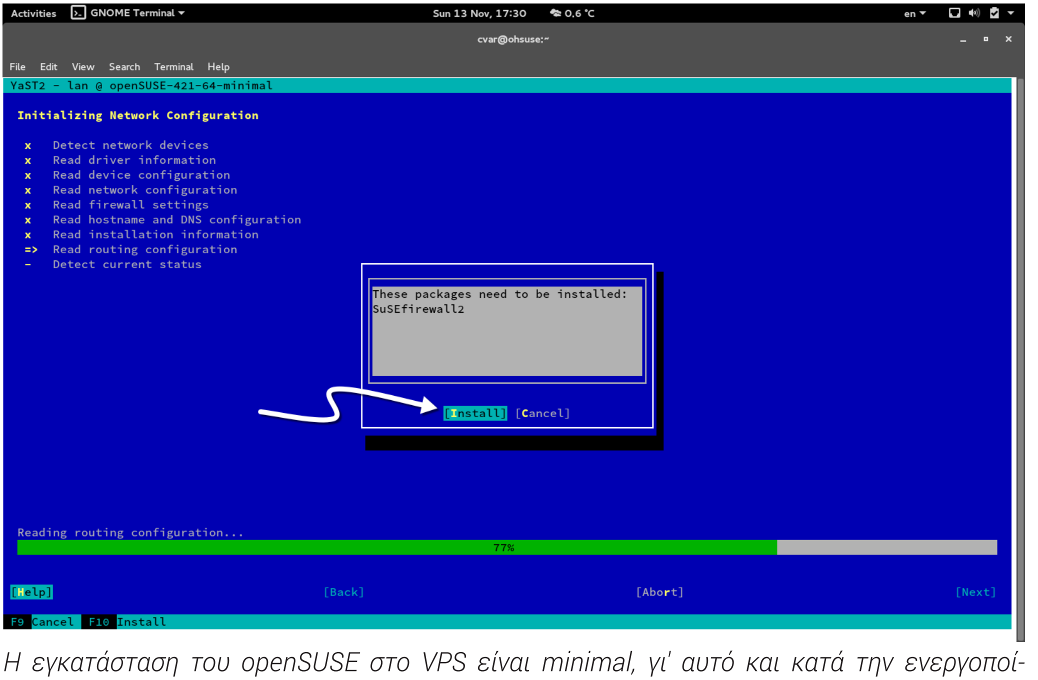
Θα παρατηρήσετε ότι το prompt του VPS εμπεριέχει το όνομα και την έκδοση του λειτουργικού (openSUSE 42.1), την εκδοχή του (64bit), καθώς και το είδος της εγκατάστασης (minimal). Στην πραγματικότητα, το prompt είναι ίδιο με το hostname του μηχανήματος:

```
openSUSE-421-64-minimal:~ # hostname
openSUSE-421-64-minimal
```

Αν θέλετε να αλλάξετε το hostname (εμείς θέλαμε), ένας τρόπος για να το πετύχετε είναι με τη βοήθεια του YaST. Εδώ πλέον δεν είναι Ubuntu, στη διάθεσή μας έχουμε ένα πανίσχυρο αλλά και βολικό εργαλείο διαχείρισης συστήματος, οπότε γιατί να μην το χρησιμοποιούμε σε κάθε ευκαιρία; Το module του YaST που θα μας εξυπηρετήσει είναι το lan, οπότε πληκτρολογούμε:

```
openSUSE-421-64-minimal:~ # yast lan
```

Κατά την αρχικοποίηση του module θα σας ζητηθεί άδεια για την εγκατάσταση του πακέτου SuSEfirewall2. Δώστε την, αφού σε λίγο θα χρειαστεί να ρυθμίσουμε και το firewall του VPS – ξανά με τη βοήθεια του αντίστοιχου module του YaST.



Η εγκατάσταση του openSUSE στο VPS είναι minimal, γι' αυτό και κατά την ενεργοποίηση του YaST module ονόματι lan μάς ζητείται άδεια για την εγκατάσταση του πακέτου SuSEfirewall2. Προτείνεται να τη δώσουμε.

Στο text interface του YaST μετακινούμαστε από στοιχείο σε στοιχείο με χρήση του πλήκτρου [Tab], των πλήκτρων του δρομέα ή με τον κατάλληλο συνδυασμό πλήκτρων. Για παράδειγμα, εμείς τώρα θέλουμε να πάμε στην κατηγορία Hostname/DNS και γι' αυτό πατάμε το συνδυασμό πλήκτρων [ALT+S]. Για τον κατάλληλο συνδυασμό ανά περίπτωση, απλά παρατηρήστε τους κίτρινους χαρακτήρες. Στην κατηγορία Hostname/DNS, δίνουμε:

- **[ALT+T]** και σβήνουμε το υπάρχον hostname, πληκτρολογώντας στη θέση του το επιθυμητό (εμείς γράψαμε vatnajokull)
- **[ALT+D]** και πληκτρολογούμε ένα domain name (εμείς δώσαμε colder.xyz)
- **[ALT+I]** και για το Modify DNS configuration επιλέγουμε το Only Manually
- **[ALT+O]** για την επικύρωση των αλλαγών.

Το YaST θα κάνει ό,τι προβλέπεται και θα τερματιστεί. Προκειμένου να εφαρμοστούν οι αλλαγές για το domain name ανοίγουμε το αρχείο /etc/resolv.conf και πάνω από τους nameservers προσθέτουμε τη γραμμή `search colder.xyz`. Φυσικά, στη θέση του `colder.xyz` εσείς θα βάλετε το δικό σας domain name. Δείτε τα περιεχόμενα του /etc/resolv.conf από το VPS μας:

```
### Hetzner Online GmbH installimage
# nameserver config
search colder.xyz
nameserver 213.133.100.100
nameserver 213.133.99.99
nameserver 213.133.98.98
nameserver 2a01:4f8:0:a0a1::add:1010
nameserver 2a01:4f8:0:a102::add:9999
nameserver 2a01:4f8:0:a111::add:9898
```

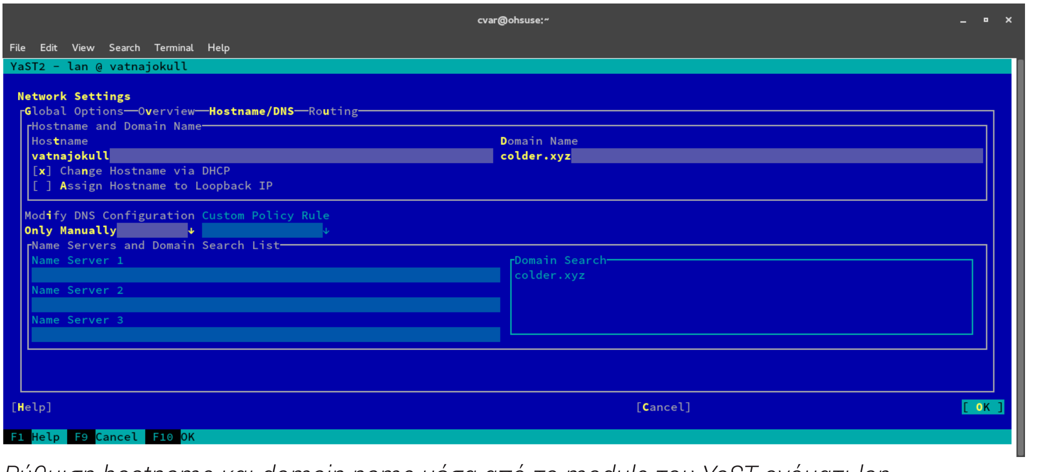
Για να τσεκάρετε ότι οι αλλαγές εφαρμόστηκαν, αποσυνδεθείτε από το VPS, συνδεθείτε και πάλι, παρατηρήστε το prompt και χρησιμοποιήστε το εργαλείο hostname (μία φορά σκέτο κι άλλη μία με την παράμετρο -f).

Αναβάθμιση πακέτων και πυρήνα

Αρχικά φρεσκάρουμε την τοπική βάση με τα περιεχόμενα των απομακρυσμένων αποθετηρίων (repositories). Λόγω της εγκατάστασης του SuSEfirewall2, η οποία έγινε πριν λίγο από πλευράς YaST, το φρεσκάρισμα είναι μάλλον περιττό αυτή τη στιγμή. Καλού κακού όμως το επαναλαμβάνουμε:

```
vatnajokull:~ # zypper ref
```

```
Repository 'openSUSE-42.1-0' is up to date.
Repository 'openSUSE-Leap-42.1-Oss' is up to date.
Repository 'openSUSE-Leap-42.1-Update' is up to date.
Repository 'openSUSE-Leap-42.1-Update-Non-Oss' is up to date.
All repositories have been refreshed.
```



Ρύθμιση hostname και domain name μέσα από το module του YaST ονόματι lan.

Πράγματι, οι πληροφορίες περί των repositories ήταν ενημερωμένες – ή τουλάχιστον αυτό συνέβη στην περίπτωσή μας. Για να δούμε τώρα αν υπάρχουν πακέτα που χρειάζονται αναβάθμιση, απλά γράφουμε:

```
vatnajokull:~ # zypper lu
```

Θα διαπιστώσετε ότι, πράγματι, ενημερωμένες εκδόσεις πακέτων υπάρχουν – και μάλιστα είναι ουκ ολίγες. Η διαδικασία της αναβάθμισης ξεκινά πληκτρολογώντας:

```
vatnajokull:~ # zypper patch
```

Ίσως διαπιστώσετε ότι πρόκειται ν' αναβαθμιστεί το ίδιο το zypper, καθώς και κάποιες συνοδευτικές βιβλιοθήκες. Απαντήστε καταφατικά στην ερώτηση για αναβάθμιση κι όταν η διαδικασία ολοκληρωθεί δώστε και πάλι `zypper patch`. Τη δεύτερη φορά θα δείτε ότι πολλά περισσότερα πακέτα πρόκειται ν' αναβαθμιστούν. Αν πρόκειται ν' αναβαθμιστεί κι ο πυρήνας, θα πάρετε μήνυμα που προτρέπει για επανεκκίνηση του συστήματος αμέσως μετά την αναβάθμιση. Σας συστήνουμε να μην την καθυστερήσετε.

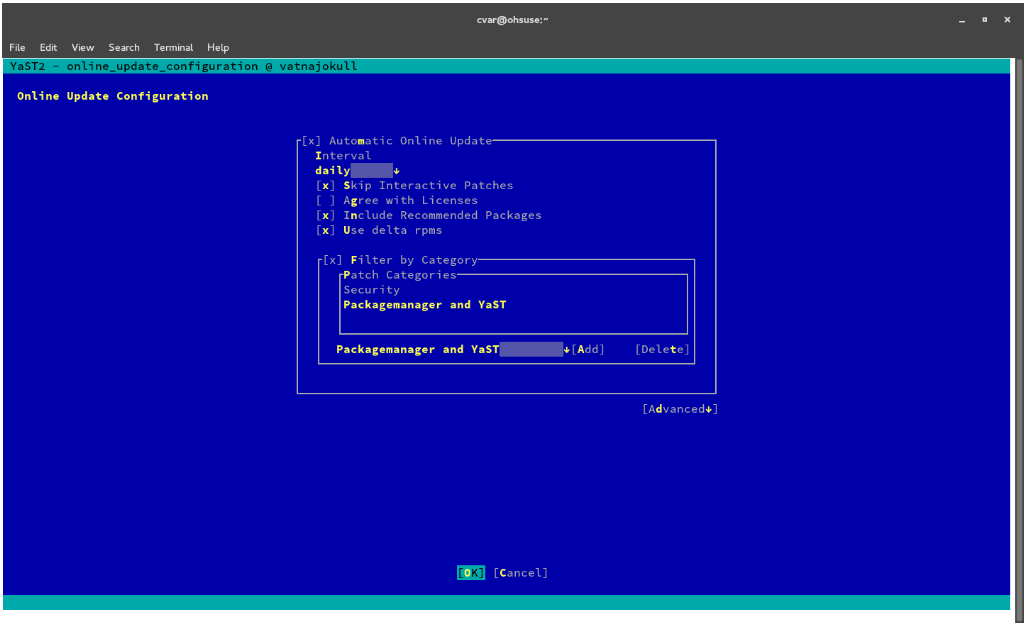
Είναι εξάλλου καλή ιδέα να ρυθμίσουμε το openSUSE ώστε, περιοδικά κι αυτόματα, να κατεβάζει και να εφαρμόζει τυχόντα διαθέσιμα updates – και κατά νου έχουμε κυρίως τα updates που αφορούν στην ασφάλεια. Για άλλη μια φορά θα προσφύγουμε στο YaST, αλλά πρώτα θα εγκαταστήσουμε το σχετικό module:

```
vatnajokull:~ # zypper -n in yast2-online-update-configuration
```

Αμέσως μετά το φορτώνουμε

```
vatnajokull:~ # yast online_update_configuration
```

κι από το text interface του κάνουμε τις επιλογές μας. (Ναι, το όνομα του πακέτου έχει παύλες αλλά το όνομα του module έχει underscores.) Δείτε το screenshot που ακολουθεί, διαβάστε φυσικά και τη συνοδευτική περιγραφή.



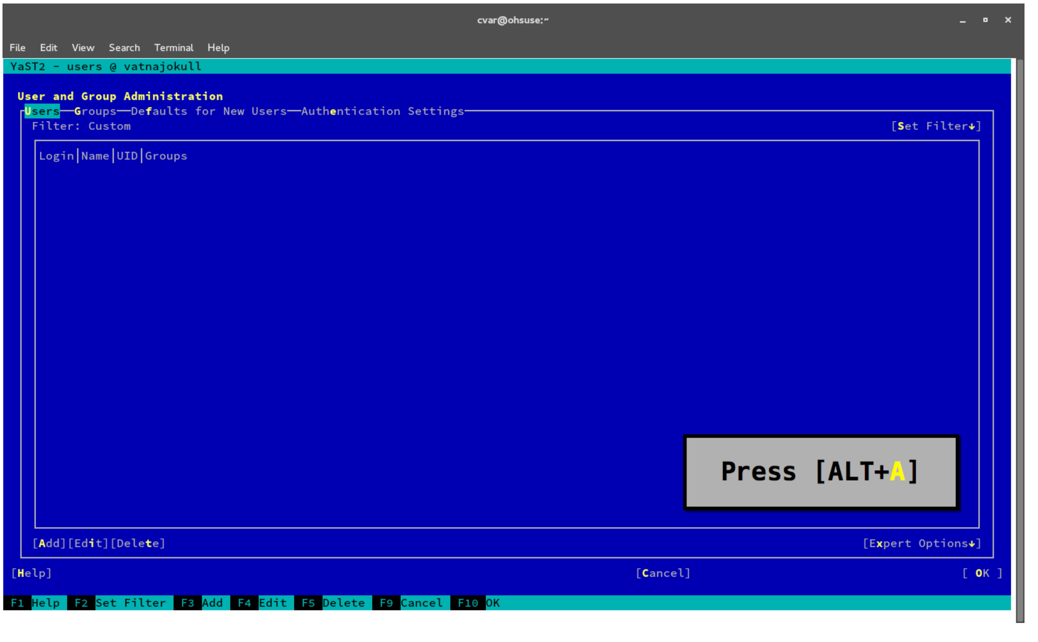
Στο συγκεκριμένο παράδειγμα φροντίζουμε ώστε κάθε μέρα να γίνεται αυτόματος έλεγχος για ενημερώσεις. Τα patches που η εγκατάστασή τους απαιτεί αλληλεπίδραση με το χρήστη τα προσπερνάμε, επιλέγουμε να μην αποδεχόμαστε αυτομάτως τις άδειες χρήσης, θέλουμε να συμπεριλαμβάνονται τα όποια προτεινόμενα updates, ενώ για οικονομία bandwidth επιδιώκουμε τη χρήση delta RPMs. Τέλος, δεν επιθυμούμε να εγκαθίστανται αυτόματα ενημερώσεις για κάθε κατηγορία πακέτων, αλλά μόνο γι' αυτά που αφορούν στον package manager και στο YaST, βεβαίως και για εκείνα που αφορούν στην ασφάλεια.

Δημιουργία νέου λογαριασμού χρήστη με δικαιώματα διαχειριστή

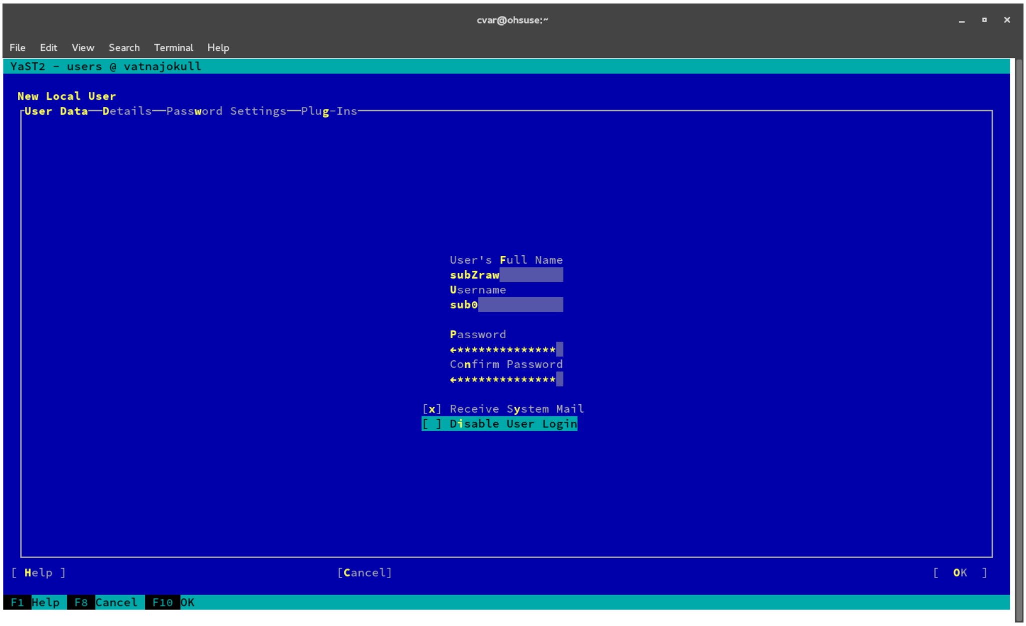
Έως αυτή τη στιγμή εργαζόμασταν από το λογαριασμό του root. Γενικά, αυτό πρέπει να το αποφεύγουμε. Για λόγους ασφαλείας –αλλά και προστασίας του συστήματος από τους ίδιους μας τους εαυτούς– καλό είναι να δημιουργήσουμε ένα λογαριασμό απλού χρήστη και να συνδεόμαστε σ' αυτόν. Ο συγκεκριμένος χρήστης θα έχει δυνατότητα για εκτέλεση εργασιών με δικαιώματα root, με τη βοήθεια του sudo. Έτσι, τις δυνατότητες του root θα τις έχουμε μόνον όποτε τις χρειαζόμαστε και για λίγο χρόνο. Την περισσότερη ώρα θα βρισκόμαστε στο λογαριασμό του απλού μας χρήστη, μέσα από τον οποίο δεν είναι εύκολο να καταλύουμε την ασφάλεια του συστήματος, βεβαίως ούτε και να φέρνουμε τα πάνω κάτω και γενικά να τα κάνουμε όλα μαντάρα. Κατά τα αναμενόμενα, το νέο λογαριασμό χρήστη θα τον δημιουργήσουμε με τη βοήθεια του YaST:

```
vatnajokull:~ # yast users
```

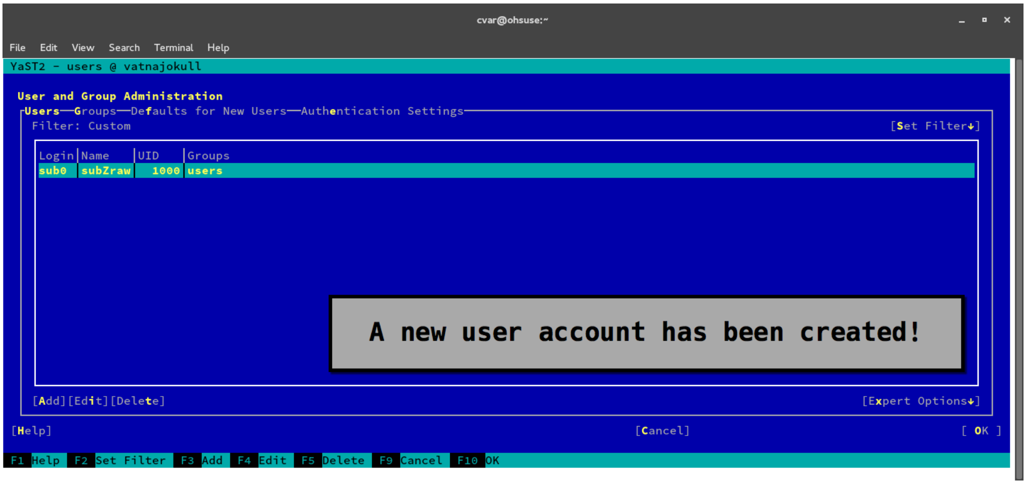
Δείτε τα τρία screenshots που ακολουθούν.



Στην κατηγορία Users επιβεβαιώνουμε ότι δεν υπάρχει κάποιος λογαριασμός απλού χρήστη στο σύστημα. Για να προσθέσουμε νέο λογαριασμό πατάμε το συνδυασμό πλήκτρων [ALT+A].



Πληκτρολογούμε στη συνέχεια το πλήρες όνομα, το username και βεβαίως το password (δύο φορές) για το λογαριασμό του νέου χρήστη. Τσεκάρουμε το Receive System Mail, ώστε τα emails που στέλνουν οι υπηρεσίες του συστήματος στον root να φτάνουν στο νέο μας χρήστη. Το Disable User Login δεν το τσεκάρουμε, αφού θέλουμε να είμαστε σε θέση να συνδεόμαστε αλληλεπιδραστικά στο λογαριασμό. Επικυρώνουμε τις ενέργειές μας με ένα [ALT+O].

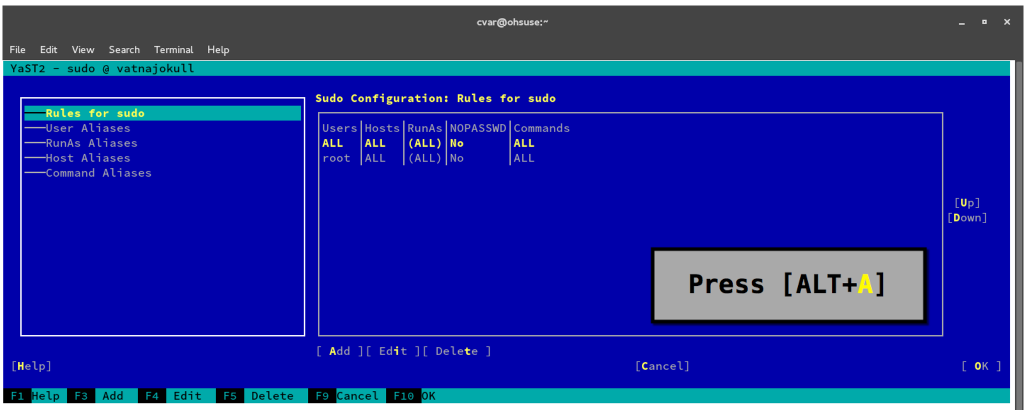


Ο νέος λογαριασμός είναι έτοιμος. Είναι του χρήστη με username το sub0, ο οποίος ανήκει στο group ονόματι users.

Θέλουμε τώρα ο νέος μας χρήστης να μπορεί και να εκτελεί εργασίες με δικαιώματα root, καθώς και να το πετυχαίνει αυτό με τη βοήθεια του εργαλείου sudo (όπως στο Ubuntu, ξέρετε). Προς τούτο, φορτώνουμε στο YaST το module με όνομα sudo:

```
vatnajokull:~ # yast sudo
```

Θα τροποποιήσουμε τους κανόνες που ισχύουν για το sudo, ειδικά όσον αφορά στο χρήστη sub0. Δείτε, παρακαλούμε πολύ, τα screenshots που ακολουθούν.

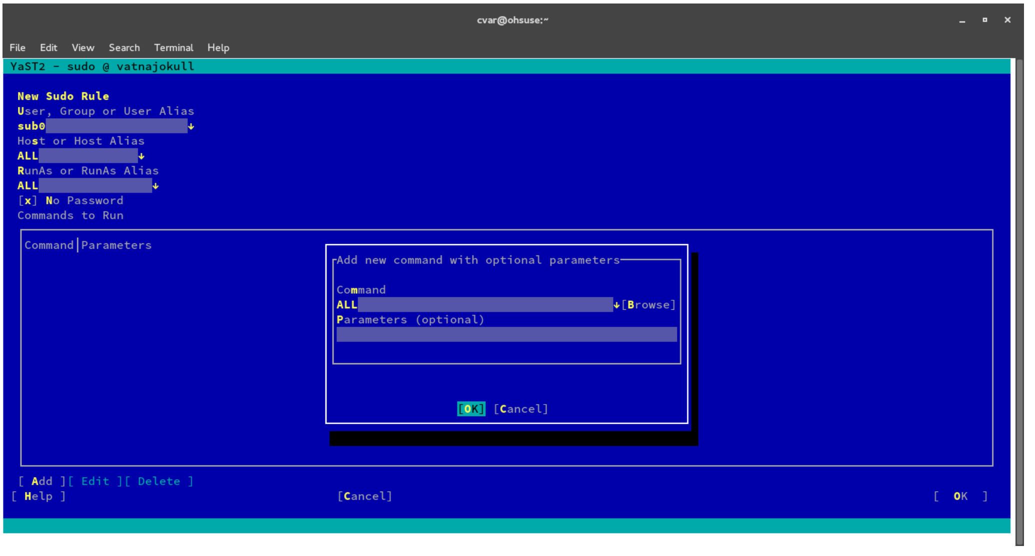


Ξεκινάμε εστιάζοντας στην κατηγορία Rules for sudo. Θέλουμε να προσθέσουμε ένα νέο κανόνα για τον χρήστη με username το sub0. Πατάμε, λοιπόν, το συνδυασμό πλήκτρων [CTRL+A].

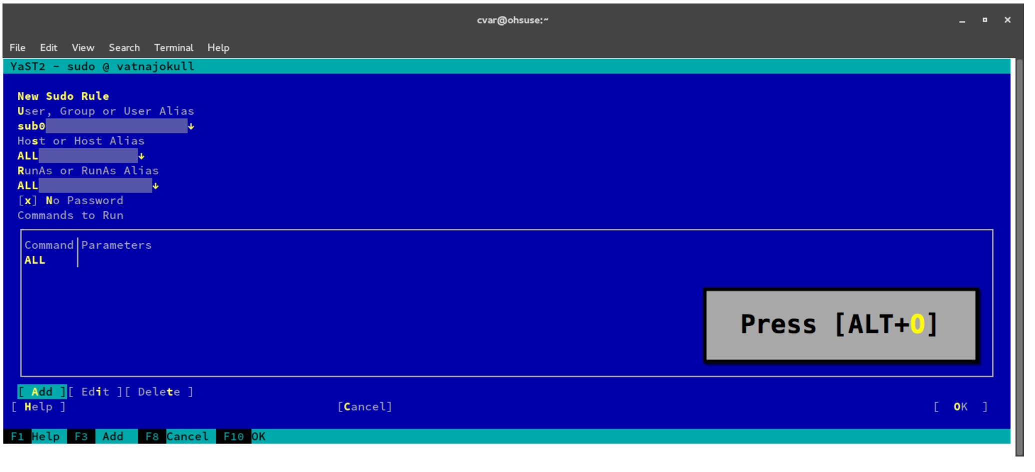


Επιλέγουμε το username του χρήστη που μας ενδιαφέρει και φροντίζουμε ώστε Host or Host Alias = RunAs or RunAs Alias = ALL. Επιθυμούμε εξάλλου να μη χρειάζεται πληκτρο-

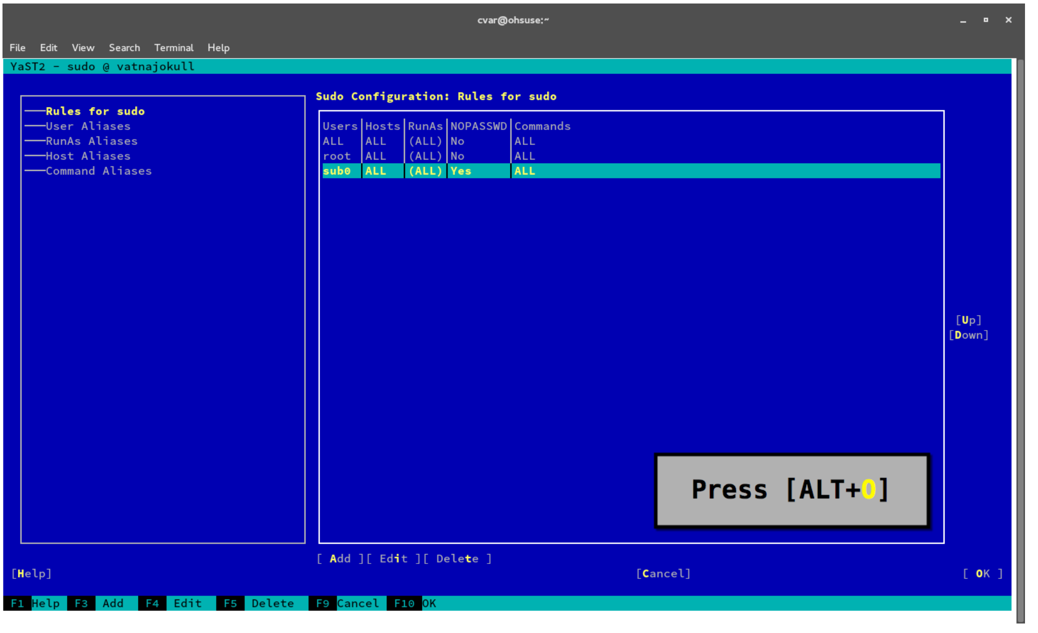
λόγηση password για τον sub0 (τσεκ στο No Password), κάθε φορά που χρησιμοποιεί το sudo. Σε λίγο άλλωστε θα φροντίσουμε ώστε στο λογαριασμό του sub0 να γίνεται σύνδεση μόνο με SSH key-based authentication. Έτσι, αν το ιδιωτικό μας κλειδί είναι προστατευμένο –όπως οφείλει να είναι–, προστατευμένος θα 'ναι κι ο λογαριασμός του sub0. Δεν έχουμε τελειώσει με το νέο κανόνα για το sudo. Για τη συνέχεια πατάμε [ALT+A].



Στο pop-up που εμφανίζεται φροντίζουμε ώστε Command = ALL και μετά πατάμε το συνδυασμό πλήκτρων [ALT+O].



Ιδού οι παράμετροι του νέου κανόνα...



...και ιδού κι όλοι οι κανόνες για το sudo. Αν είμαστε ικανοποιημένοι με τη δουλειά μας, παγιώνουμε τις αλλαγές με [ALT+O].

Πριν συνεχίσουμε αξίζει να βεβαιωθούμε ότι ο νέος κανόνας για το sudo δουλεύει σωστά, μ' άλλα λόγια ότι μας δίνει προσωρινά δικαιώματα root και μάλιστα χωρίς να πληκτρολογούμε κάποιο password:

```
sub0@vatnajokull:~> sudo ls -lha /root
total 32K
drwx------  6 root root 4.0K Nov 15 23:45 .
drwxr-xr-x 22 root root 4.0K Nov  6 14:33 ..
-rw-------  1 root root 2.6K Nov 15 23:46 .bash_history
drwx------  3 root root 4.0K Nov 14 06:46 .config
drwx------  2 root root 4.0K Sep 30  2015 .gnupg
drwxr-xr-x  3 root root 4.0K Feb 23  2016 .local
drwx------  2 root root 4.0K Feb 23  2016 .ssh
-rw-------  1 root root 2.9K Nov 15 23:45 .viminfo
```

Όταν είναι απαραίτητο να βρισκόμαστε στο λογαριασμό του root, μπορούμε να μεταβαίνουμε σ' αυτόν πληκτρολογώντας

```
sub0@vatnajokull:~> sudo su
```

Βελτίωση ασφάλειας για απομακρυσμένες συνδέσεις

Στο σημείο αυτό έχουμε δύο χρήστες στο σύστημα, τον root και τον sub0 — ή όπως αλλιώς είναι το username του δικού σας. Σε κάθε λογαριασμό συνδεόμαστε μέσω SSH πληκτρολογώντας το αντίστοιχο password. Για λόγους ασφαλείας θα ρυθμίσουμε τον OpenSSH server ώστε η μοναδική αποδεκτή μέθοδος authentication να 'ναι αυτή που βασίζεται στα δημόσια κλειδιά SSH. Επιπρόσθετα, η απευθείας σύνδεση μέσω SSH στο λογαριασμό του root θα απαγορεύεται.

Οφείλουμε πρώτα να μεταφέρουμε στο VPS το δημόσιο κλειδί SSH του τοπικού μας χρήστη — συγκεκριμένα θα το προσθέσουμε στο αρχείο .ssh/authorized_keys του (απομακρυσμένου) sub0. Το τι σημαίνει αυτό, πώς επιτυγχάνεται και πολλά περισσότερα για το SSH key-based authentication, μπορείτε να διαβάσετε στο https://deltahacker.gr/?p=13357. Μετά τη μεταφορά, στο λογαριασμό του sub0 θα συνδεόμαστε μέσω SSH και χωρίς την πληκτρολόγηση του αντίστοιχου password. Προσοχή, όμως: Αυτό θα είναι δυνατόν μόνον εφόσον ξεκινάμε τη σύνδεση από τον τοπικό λογαριασμό του χρήστη, το δημόσιο κλειδί του οποίου έχουμε μεταφέρει. Πριν προχωρήσουμε, λοιπόν, καλό θα ήταν να μεταφέρουμε στο VPS τα δημόσια κλειδιά κι άλλων χρηστών μας, από άλλα μηχανήματά μας. Μια ιδέα είναι να έχουμε όλα τα δημόσια κλειδιά κάπου στο cloud, π.χ., στο Dropbox ή σε μια εγκατάσταση του ownCloud, και να τα κατεβάζουμε στο VPS που θέλουμε, π.χ., με τη βοήθεια του wget.

Ας ρυθμίσουμε τώρα τον OpenSSH server στο VPS μας. Με δικαιώματα διαχειριστή (sudo) ανοίγουμε το αρχείο /etc/ssh/sshd_config με τον editor της προτίμησής μας:

```
sub0@vatnajokull:~> sudo vi /etc/ssh/sshd_config
```

Αν δεν πολυσυμπαθείτε το vi χρησιμοποιήστε το nano (εγκαταστήστε το με ένα sudo zypper -n in nano). Στο sshd_config φροντίζουμε ώστε:

- το `PermitRootLogin yes` να γίνει `PermitRootLogin no`
- το `#PubkeyAuthentication yes` να γίνει `PubkeyAuthentication yes`
- το `PasswordAuthentication yes` να γίνει `PasswordAuthentication no`
- το `#ChallengeResponseAuthentication` yes να γίνει `ChallengeResponseAuthentication no`.

Αποθηκεύουμε τις αλλαγές, εγκαταλείπουμε τον editor κι αναγκάζουμε τον OpenSSH server να λάβει υπόψη τις αλλαγές:

```
sub0@vatnajokull:~> sudo systemctl reload sshd.service
```

Πολύ ωραία. Αν όλα έγιναν σωστά, τώρα θα πρέπει να είμαστε σε θέση για απομακρυσμένες συνδέσεις στο λογαριασμό του sub0 *χωρίς* την πληκτρολόγηση password. Επιχειρώντας εξάλλου σύνδεση στο λογαριασμό του root, θα παίρνουμε μήνυμα λάθους. Παράδειγμα:

```
cvar@ohsuse:~> ssh root@vatnajokull.colder.xyz
Permission denied (publickey).
```

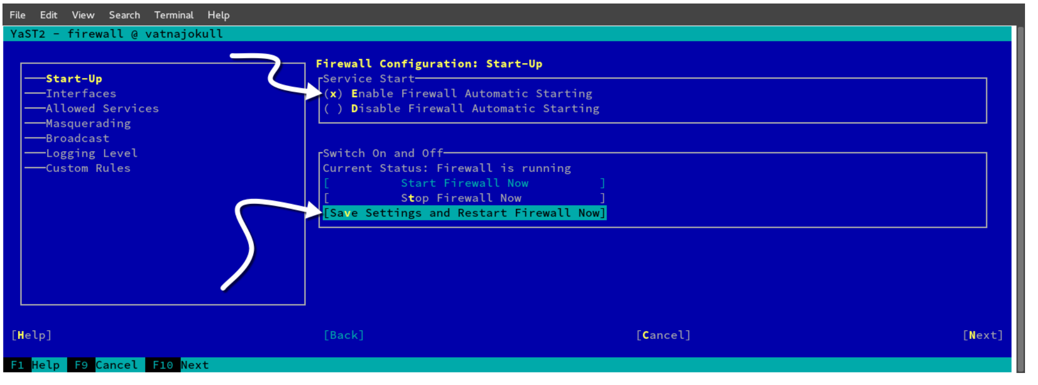
Ακόμη κι αν μεταφέρουμε το κατάλληλο δημόσιο κλειδί στο αρχείο .ssh/authorized_keys του root, εξαιτίας της οδηγίας `PermitRootLogin no` στο /etc/ssh/sshd_config η απευθείας απομακρυσμένη πρόσβαση θα συνεχίσει να απαγορεύεται.

Ρύθμιση κι ενεργοποίηση firewall

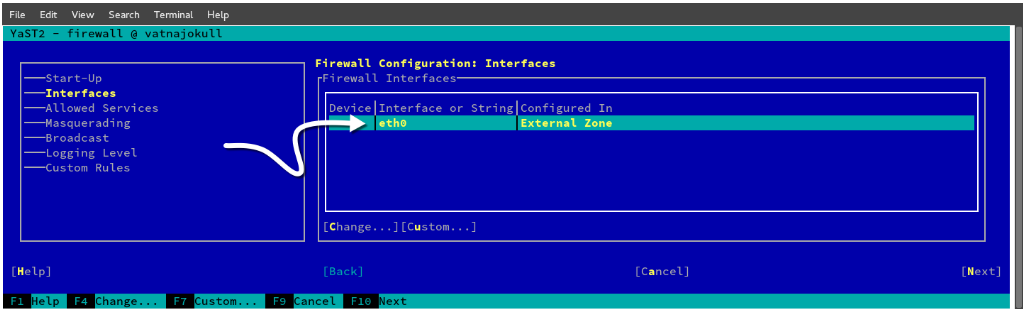
Στο VPS μας δεν υπάρχει τείχος προστασίας ενεργοποιημένο, αλλά αυτό αλλάζει εύκολα. Από το λογαριασμό του απλού μας χρήστη, πληκτρολογούμε:

```
sub0@vatnajokull:~> sudo yast2 firewall
```

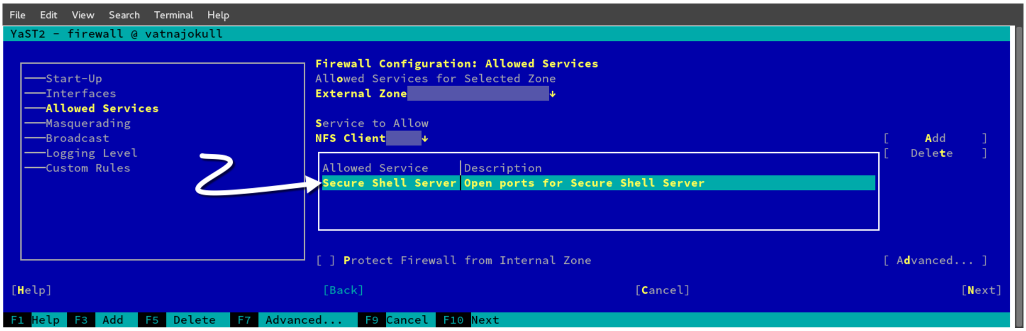
Δείτε τα screenshots που ακολουθούν και διαβάστε τις αντίστοιχες περιγραφές.



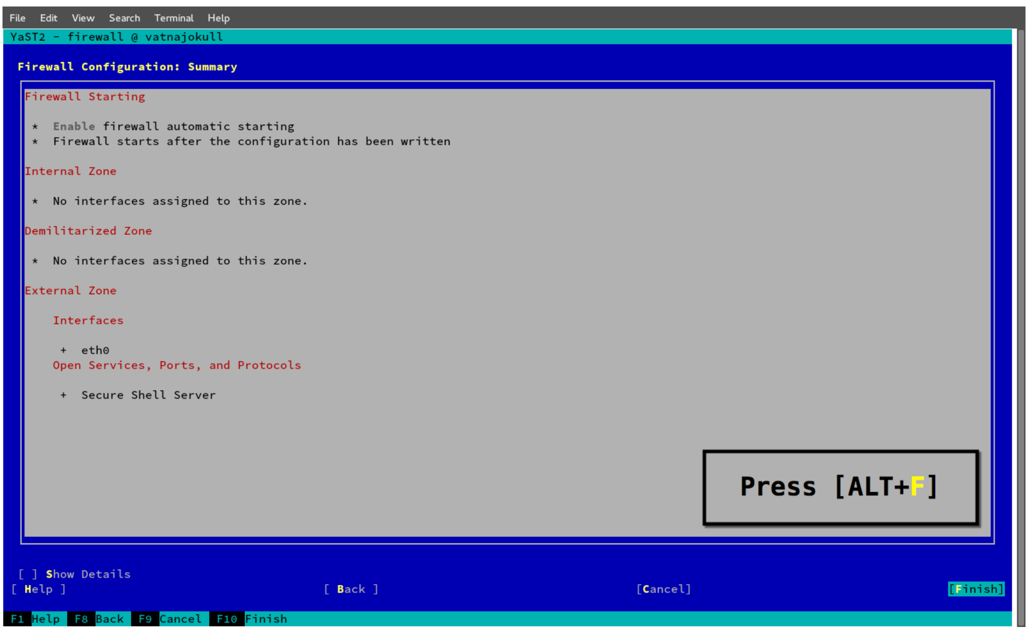
Θέλουμε το firewall να ενεργοποιείται με την εκκίνηση του λειτουργικού, γι' αυτό και στην κατηγορία ρυθμίσεων Start-Up (βλ. αριστερά) φροντίζουμε ώστε να είναι επιλεγμένο το Enable Firewall Automatic Starting. Το θέλουμε επίσης ενεργό και τώρα, οπότε πηγαίνουμε πάνω από το Start Firewall Now και πατάμε το [Enter].



Στην κατηγορία ρυθμίσεων Interfaces φροντίζουμε ώστε το eth0, το οποίο είναι το ένα και μοναδικό network interface του VPS μας, να ανήκει στο External Zone.



Πηγαίνουμε μετά στην κατηγορία Allowed Services. Πρόκειται να υποδείξουμε τις δικτυακές υπηρεσίες στις οποίες θα επιτρέπεται πρόσβαση από τον έξω κόσμο. Αρχικά, για το Allowed Services for Selected Zone επιλέγουμε το External Zone. Για το Services to Allow διαλέγουμε το Secure Shell Server και πατάμε [ALT+A]. Μόλις υποδείξαμε ότι θέλουμε να επιτρέπονται οι συνδέσεις στον OpenSSH server από το Internet, αλλά σε καμία άλλη υπηρεσία. Πατάμε [ALT+N] για το επόμενο και τελευταίο βήμα.



Στο κεντρικό πλαίσιο βλέπουμε όλες τις επιλογές κι αλλαγές που πρόκειται να εφαρμοστούν. Ρίξτε μια ματιά και βεβαιωθείτε ότι: (α) το firewall θα ξεκινά αυτόματα κατά το boot του openSUSE, (β) θα ενεργοποιηθεί αμέσως μετά την έξοδό μας από το YaST, (γ) θα επιτρέπει τις συνδέσεις στον OpenSSH server από το Internet, (δ) θα απαγορεύει τις συνδέσεις οπουδήποτε αλλού. Πατάμε [ALT+F] για την εφαρμογή των αλλαγών.

Ένας τρόπος για να βεβαιωθούμε ότι το firewall λειτουργεί όπως θέλουμε, είναι να επανεκκινήσουμε το VPS

```
sub0@vatnajokull:~> sudo reboot
```

κι αφού φορτώσει να κάνουμε ένα port scanning, π.χ., με τη βοήθεια του nmap. Δείτε το ακόλουθο παράδειγμα, όπου σκανάρουμε το vatnajokull.colder.xyz από το τερματικό ενός MacBook:

```
mbpr15:~ cvar$ sudo nmap -sS -sV -O -p1-65535 vatnajokull.colder.xyz
Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-19 09:52 CET
Nmap scan report for vatnajokull.colder.xyz (88.99.14.133)
Host is up (0.026s latency).
Not shown: 65533 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 6.6.1 (protocol 2.0)
3544/tcp closed teredo
Device type: WAP|general purpose|media device|phone
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (91%), Linksys embedded (91%), 
Google Android 4.X (85%)
OS CPE: cpe:/o:linux:linux_kernel cpe:/h:linksys:ea3500 cpe:/o:linux:linux_
kernel:3.13 cpe:/o:linux:linux_kernel:4.2 cpe:/o:linux:linux_kernel:3.x cpe:/
o:linux:linux_kernel:2.6 cpe:/o:google:android:4.0
Aggressive OS guesses: Linksys EA3500 WAP (91%), Linux 3.13 or 4.2 (86%), Linux 
3.2 - 4.4 (86%), XBMCbuntu Frodo v12.2 (Linux 3.X) (85%), Linux 2.6.32 - 2.6.36 
(85%), Android 4.0 (85%)
No exact OS matches for host (test conditions non-ideal).
OS and Service detection performed. Please report any incorrect results at 
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.93 seconds
mbpr15:~ cvar$
```

Θα παρατηρήσετε ότι εκτός από το port 22/TCP, το οποίο αναμενόμενα είναι ανοικτό λόγω OpenSSH server, ανοικτό είναι και το 3544/TCP (https://en.wikipedia.org/wiki/Teredo_tunneling). Το nmap εντόπισε το εν λόγω ανοικτό port όχι επειδή το firewall του openSUSE κάνει του κεφαλιού του, αλλά διότι το δημόσιο IP του vatnajokull.colder.xyz είναι διαφορετικό από το IP που έχει το eth0 interface του VPS: έτσι είναι το μοντέλο δικτύωσης που ακολουθεί η Hetzner, η οποία για την πρόσβαση στα VPS υλοποιεί τεχνικές NAT.

Να σημειώσουμε τέλος ότι με το firewall module του YaST, που μόλις χρησιμοποιήσαμε, ουσιαστικά ρυθμίσαμε το γνωστό iptables του Linux. Προκειμένου να δούμε όλους τους κανόνες που ισχύουν για όλες τις αλυσίδες, στο τερματικό μας γράφουμε:

```
sub0@vatnajokull:~> sudo iptables -S
```

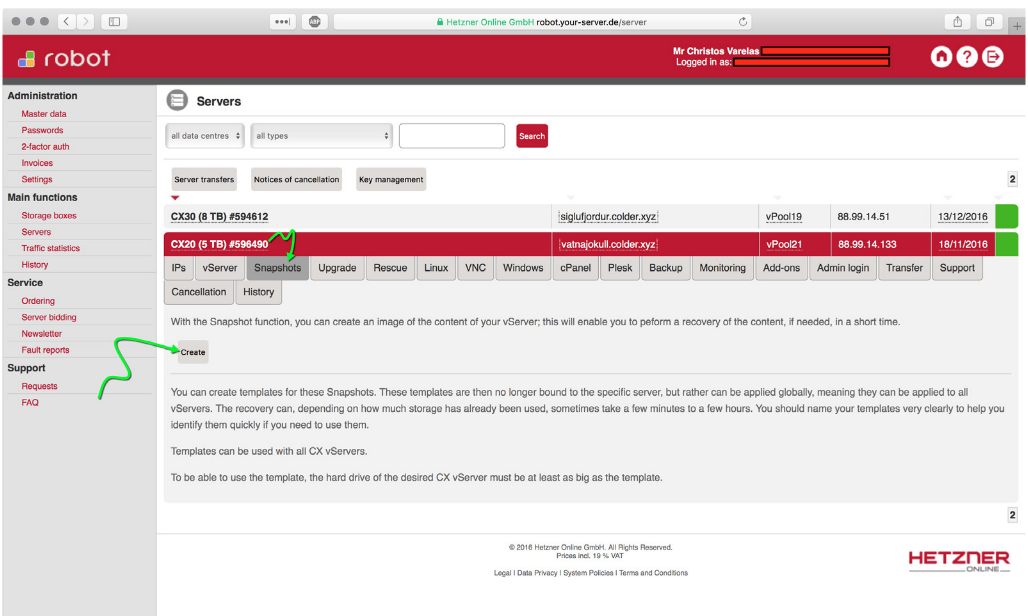
```
File  Edit  View  Search  Terminal  Help
sub0@vatnajokull:~>
sub0@vatnajokull:~> sudo iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT ACCEPT
-N forward_ext
-N input_ext
-N reject_func
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m conntrack --ctstate RELATED -j ACCEPT
-A INPUT -j input_ext
-A INPUT -m limit --limit 3/min -j LOG --log-prefix "SFW2-IN-ILL-TARGET " --log-tcp-options --log-ip-options
-A INPUT -j DROP
-A FORWARD -m limit --limit 3/min -j LOG --log-prefix "SFW2-FWD-ILL-ROUTING " --log-tcp-options --log-ip-options
-A OUTPUT -o lo -j ACCEPT
-A input_ext -m pkttype --pkt-type broadcast -j DROP
-A input_ext -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A input_ext -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A input_ext -p tcp -m limit --limit 3/min -m tcp --dport 22 --tcp-flags FIN,SYN,RST,ACK SYN -j LOG --log-prefix "SFW2-INext-ACC-TCP " --log-t
cp-options --log-ip-options
-A input_ext -p tcp -m tcp --dport 22 -j ACCEPT
-A input_ext -m pkttype --pkt-type multicast -j DROP
-A input_ext -m pkttype --pkt-type broadcast -j DROP
-A input_ext -p tcp -m limit --limit 3/min -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -j LOG --log-prefix "SFW2-INext-DROP-DEFLT " --log-tcp-optio
ns --log-ip-options
-A input_ext -p icmp -m limit --limit 3/min -j LOG --log-prefix "SFW2-INext-DROP-DEFLT " --log-tcp-options --log-ip-options
-A input_ext -p udp -m limit --limit 3/min -m conntrack --ctstate NEW -j LOG --log-prefix "SFW2-INext-DROP-DEFLT " --log-tcp-options --log-ip-
options
-A input_ext -j DROP
-A reject_func -p tcp -j REJECT --reject-with tcp-reset
-A reject_func -p udp -j REJECT --reject-with icmp-port-unreachable
-A reject_func -j REJECT --reject-with icmp-proto-unreachable
sub0@vatnajokull:~>
```

Το module του YaST ονόματι firewall μας επιτρέπει να συντάσσουμε εύκολα κανόνες για το iptables του Linux, χωρίς να είμαστε experts. Αν και προηγουμένως ορίσαμε έναν μόνο κανόνα, ώστε οι εισερχόμενες συνδέσεις στο port 22/TCP να γίνονται αποδεκτές, στην πραγματικότητα το YaST έχει κάνει αρκετή δουλειά στο παρασκήνιο.

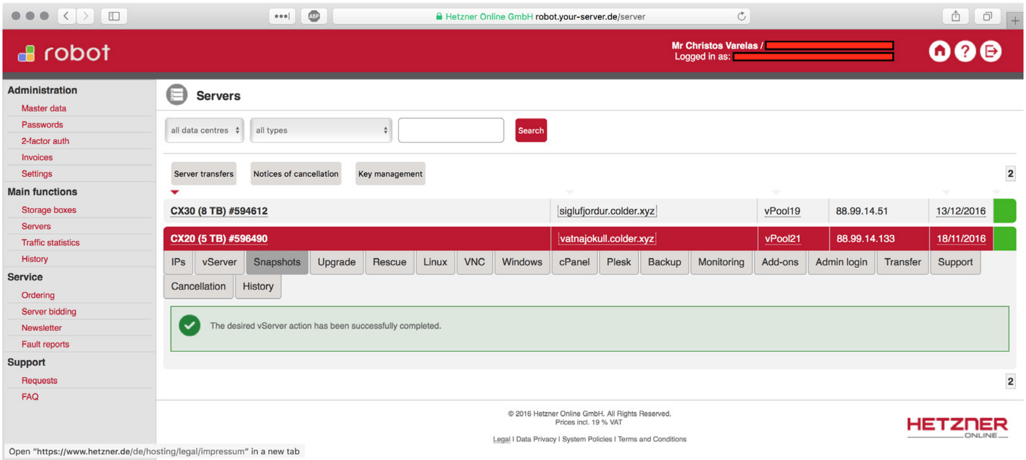
Στους κανόνες που συντάσσει το YaST θα παρατηρήσετε ότι συμπεριλαμβάνει και παραμέτρους για προστασία από όσους επιχειρούν να καταχραστούν τους πόρους του μηχανήματος. Για παράδειγμα, το firewall δεν δέχεται πάνω από τρεις απόπειρες το λεπτό για σύνδεση μέσω SSH. Από εκεί και πέρα η Hetzner υλοποιεί και τεχνικές αντιμετώπισης επιθέσεων DDoS (https://www.hetzner.de/us/hosting/unternehmen/ddos-schutz), οι οποίες μάλιστα παρέχονται χωρίς κάποια έξτρα χρέωση. Δεν έχουμε ακόμα διαπιστώσει κατά πόσο είναι αποτελεσματικές στην πράξη. Με δεδομένο πάντως ότι κατά καιρούς διάφοροι καλοθελητές τεστάρουν τις αντοχές του https://deltahacker.gr, σκεφτόμαστε πως όταν με το καλό μεταφέρουμε το site στη Hetzner δεν αποκλείεται ν' αποκτήσουμε ίδια άποψη για τους μηχανισμούς προστασίας DDoS της εταιρείας.

Προαιρετικό: Λήψη snapshot για ολόκληρο το VPS

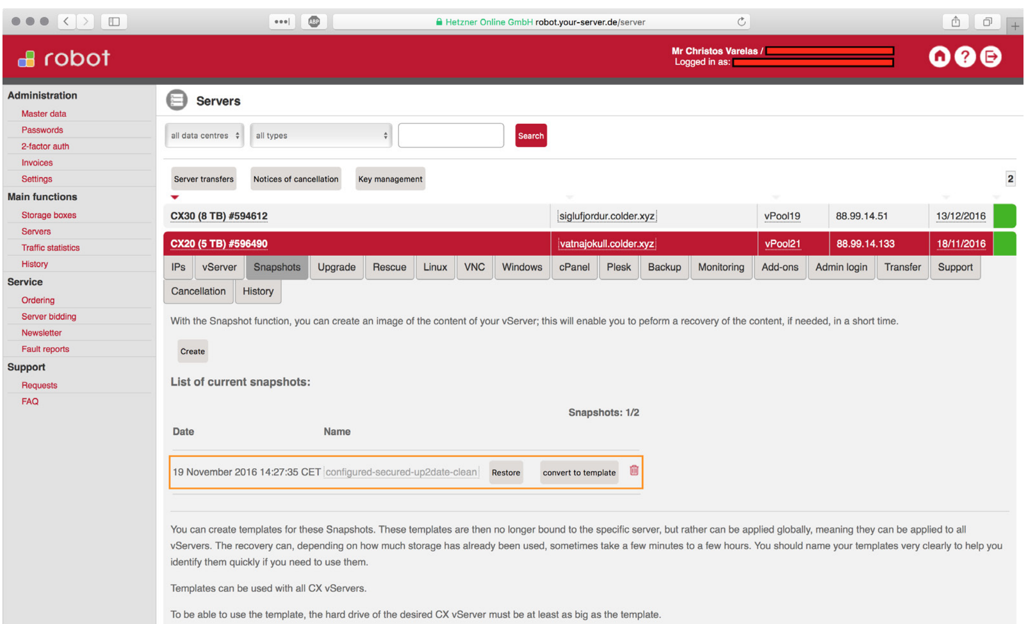
Στο σημείο αυτό θεωρούμε ότι έχουμε έναν ικανοποιητικά ασφαλή κι ευέλικτο server με openSUSE στο cloud, χωρίς να περιλαμβάνει περιττό λογισμικό και υπηρεσίες. Ουσιαστικά, είναι ό,τι πρέπει για να χτίσουμε την όποια δικτυακή εφαρμογή σχεδιάζουμε και καλό θα ήταν να μπορούσαμε να επιστρέφαμε ανά πάσα στιγμή σ' αυτό το σημείο της εξέλιξής του, π.χ., στην περίπτωση που γίνει κάποιο μπέρδεμα και τα 'χουμε κάνει μαντάρα. Αναφερόμαστε βεβαίως σ' εμάς και μόνον, φίλες και φίλοι, αφού είμαστε σίγουροι ότι εσείς δεν τα κάνετε ποτέ μαντάρα. Ευτυχώς η Hetzner επιτρέπει τη δημιουργία δύο δωρεάν snapshots για τα vServers της κατηγορίας CX20, επομένως και γι' αυτό με το οποίο δουλεύουμε στο πλαίσιο του παρόντος άρθρου. Τα snapshots δημιουργούνται κι επαναφέρονται από το web panel της Hetzner.



Για τη δημιουργία snapshot πηγαίνουμε στο web panel της Hetzner, επιλέγουμε τον vServer που μας ενδιαφέρει και, αφού βεβαιωθούμε ότι το VPS είναι powered-off, απλά κάνουμε ένα κλικ στο κουμπάκι Create.



Ύποπτα γρήγορα παίρνουμε το ακόλουθο μήνυμα: "Η επιθυμητή δράση επί του vServer ολοκληρώθηκε επιτυχώς" (ή κάπως έτσι). Είναι δυνατόν να ελήφθη τόσο γρήγορα το snapshot; Κρίνοντας εκ του αποτελέσματος, ναι, είναι.



Μετά τη λήψη του snapshot, καλό είναι να του δώσουμε ένα περιγραφικό όνομα. Για την επαναφορά ενός snapshot φροντίζουμε ώστε ο αντίστοιχος vServer να είναι κλειστός κι απλά πατάμε στο κουμπί Restore (στα δεξιά του αντίστοιχου snapshot). Παρατηρήστε εξάλλου ότι η Hetzner επιτρέπει τη μετατροπή των snapshots σε πρότυπα (templates). Ένα snapshot είναι κάτι σαν ανεξάρτητο snapshot, υπό την έννοια ότι δεν αντιστοιχίζεται σε συγκεκριμένο VPS και μπορεί ν' αναπτυχθεί "πάνω" από έναν οποιονδήποτε εικονικό server – αρκεί ο εικονικός του δίσκος να έχει μέγεθος όχι μικρότερο από μέγεθος του εικονικού δίσκου στο template.

Skill: Beginner
Tags: GParted, disk, partition, Debian

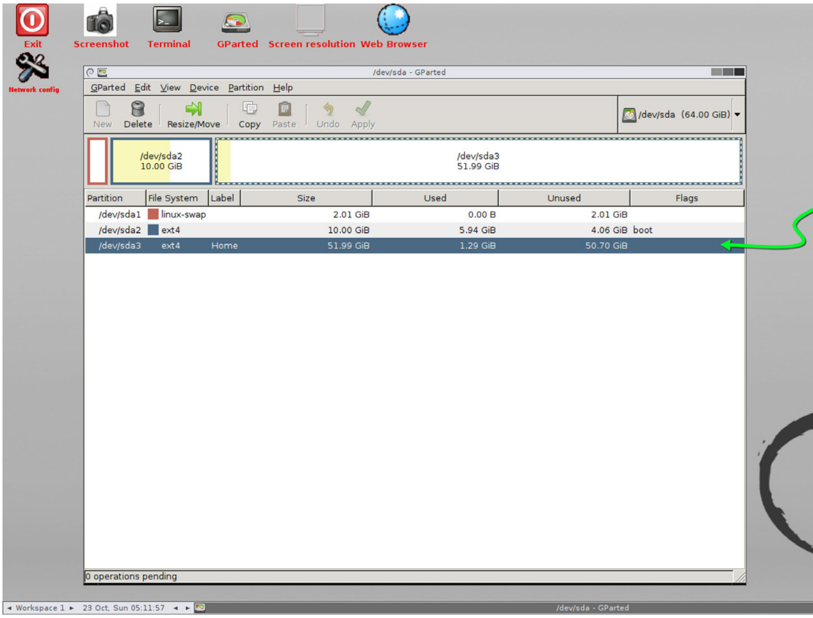
Διαχείριση κατατμήσεων με το GParted

Το GParted είναι ένα δωρεάν εργαλείο για τη διαχείριση των κατατμήσεων στους δίσκους. Χάρη στο εύχρηστο περιβάλλον γραφικών που διαθέτει, εργασίες όπως δημιουργία, αντιγραφή, μετακίνηση ή και αλλαγή μεγέθους κατατμήσεων, πραγματοποιούνται πανεύκολα και με λίγα μόλις κλικ.

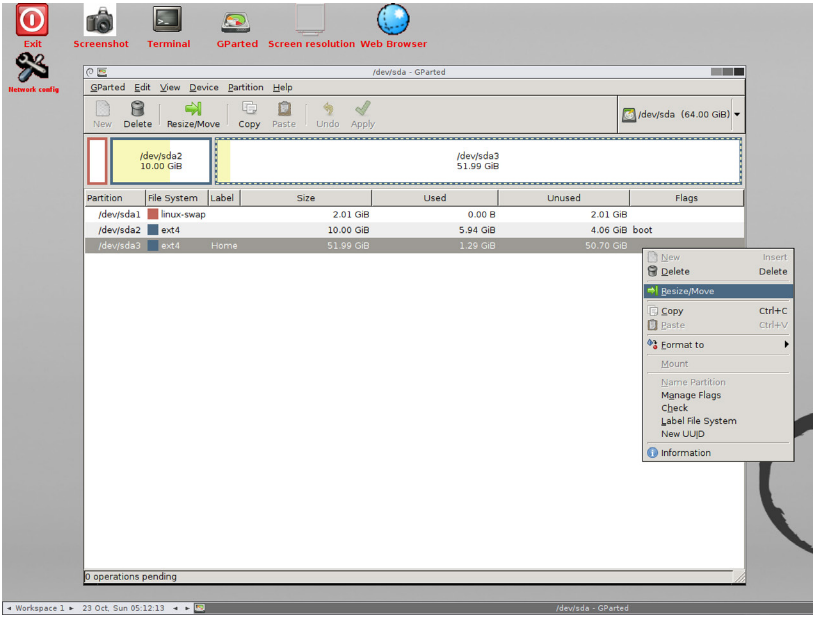
Στο πλαίσιο του άρθρου μας περί των πρακτικών κρυπτογράφησης δεδομένων στους δίσκους (σελ. 14), είδαμε μεταξύ άλλων πώς επιτυγχάνεται η μη-καταστροφική συρρίκνωση μιας υπάρχουσας κατάτμησης – και συγκεκριμένα εκείνης κάτω από το /home. Επιθυμία μας ήταν ν' αποκτήσουμε τον απαραίτητο ελεύθερο χώρο για τη δημιουργία νέας (κρυπτογραφημένης) κατάτμησης. Προκειμένου να πετύχουμε το σκοπό μας ξεκινήσαμε το openSUSE Leap σε rescue mode, συνδεθήκαμε στο λογαριασμό του root, αποπροσαρτήσαμε το home partition, το συρρικνώσαμε κατά 10GB και μετά είμασταν έτοιμοι για τη συνέχεια. Όλες τις απαραίτητες εργασίες τις φέραμε εις πέρας με το YaST, μέσα από το text interface που διαθέτει. Το εν λόγω πολυεργαλείο το βρίσκουμε αποκλειστικά στο (open)SUSE. Βεβαίως, θα ήταν δυνατόν να 'χαμε δουλέψει από οποιαδήποτε άλλη διανομή Linux κι από τη γραμμή εντολών, π.χ., καταφεύγοντας στο εργαλείο parted. Αν –λέμε, αν– κάπου σκαλώναμε, ε, γι' αυτό υπάρχουν και τα man pages.

Ορισμένες φορές πάντως θέλουμε να κάνουμε γρήγορα κι εύκολα τις εργασίες μας, χωρίς ιδιαίτερες προετοιμασίες, σχεδιασμούς και προσφυγές στο man. Αναμενόμενα, επιλογές εξακολουθούν να υπάρχουν. Για το θέμα που τώρα συζητάμε, δηλαδή για τη διαχείριση κατατμήσεων, ένα εργαλείο που λύνει τα χέρια είναι το GParted. Όπως αναγράφεται και στον επίσημο δικτυακό τόπο (http://gparted.org), το GParted τρέχει σε υπολογιστές με Linux, αρχιτεκτονικής x86 ή x86-64. Επειδή όμως διατίθεται κι ως Live CD ή Live USB, πρακτικά μπορεί να χρησιμοποιηθεί σε οποιονδήποτε υπολογιστή x86/x86-64 ανεξάρτητα του λειτουργικού του συστήματος. Το GParted Live είναι η εν λόγω Debian-based διανομή που ελεύθερα κατεβάζουμε από το http://gparted.org/download.php. Δείτε στα ακόλουθα screenshots ένα παράδειγμα χρήσης του GParted Live, το οποίο επιστρατεύουμε ώστε να συρρικνώσουμε *μη καταστροφικά* το μέγεθος μιας υπάρχουσας κατάτμησης που είναι διαμορφωμένη σε Ext4.

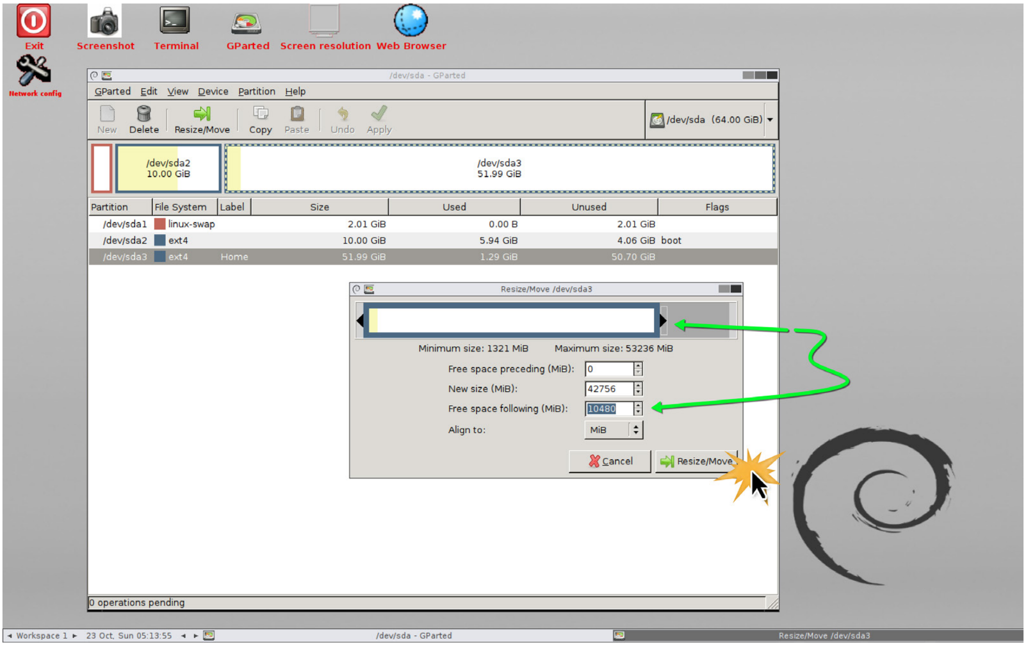
Σημείωση. Πριν τη χρήση του GParted Live προτείνεται να έχουμε πάρει ένα καλό backup της κατάτμησης ή των κατατμήσεων με τις οποίες πρόκειται να εργαστούμε. Ακόμα καλύτερο θα ήταν ένα backup ολόκληρου του δίσκου. Βέβαια το GParted είναι σταθερό κι ώριμο κι αν ξέρουμε τι κάνουμε δεν υπάρχει περίπτωση να χάσουμε δεδομένα, ποτέ όμως δεν βλάπτει να είμαστε έξτρα προσεκτικοί. (Message brought to you from the abundans-cautela-non-nocet department.)



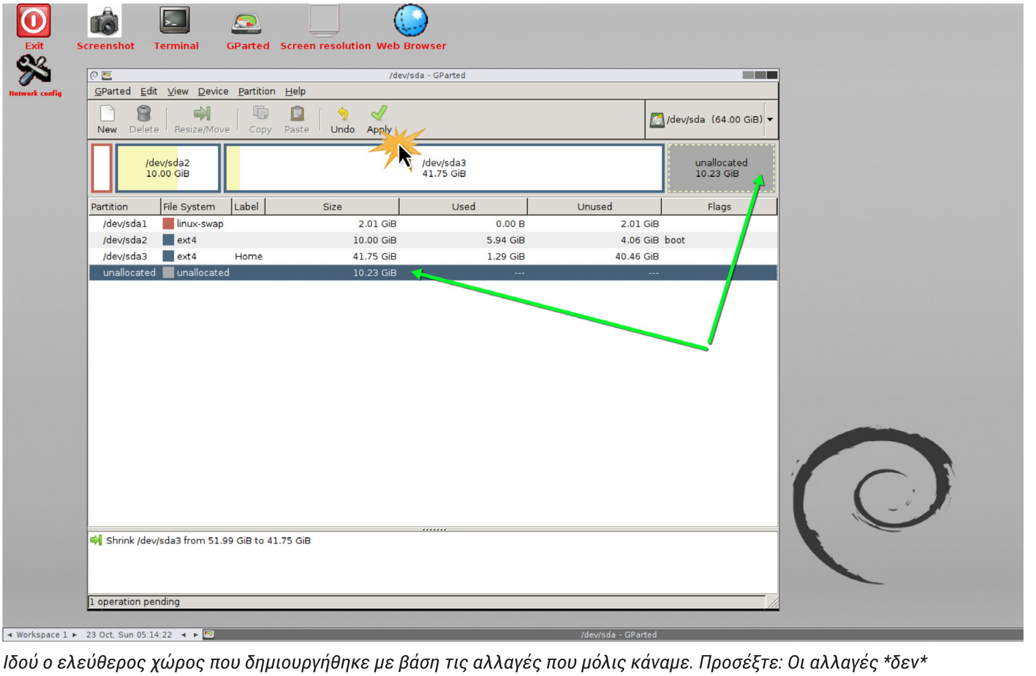
Μετά την εκκίνηση του GParted Live φορτώνει το περιβάλλον γραφικών και η εφαρμογή ξεκινά αυτόματα. Στο screenshot έχουμε ήδη επιλέξει, με κλικ πάνω της, την κατάτμηση που θέλουμε να συρρικνώσουμε.



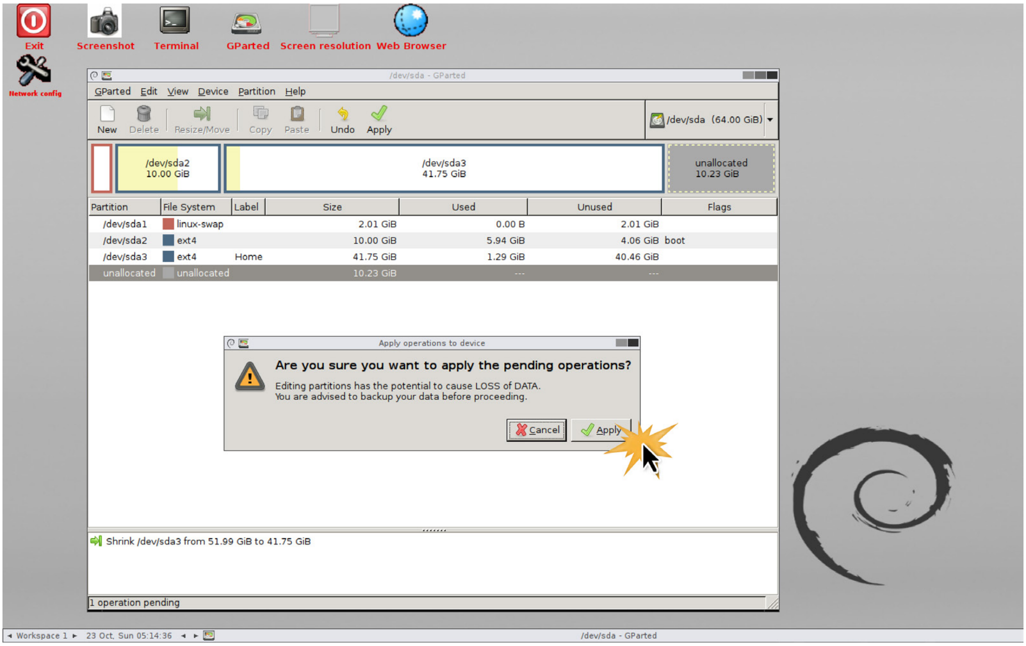
Για την αλλαγή μεγέθους κάνουμε δεξί κλικ πάνω στην επιλεγμένη κατάτμηση κι επιλέγουμε το Resize/Move.



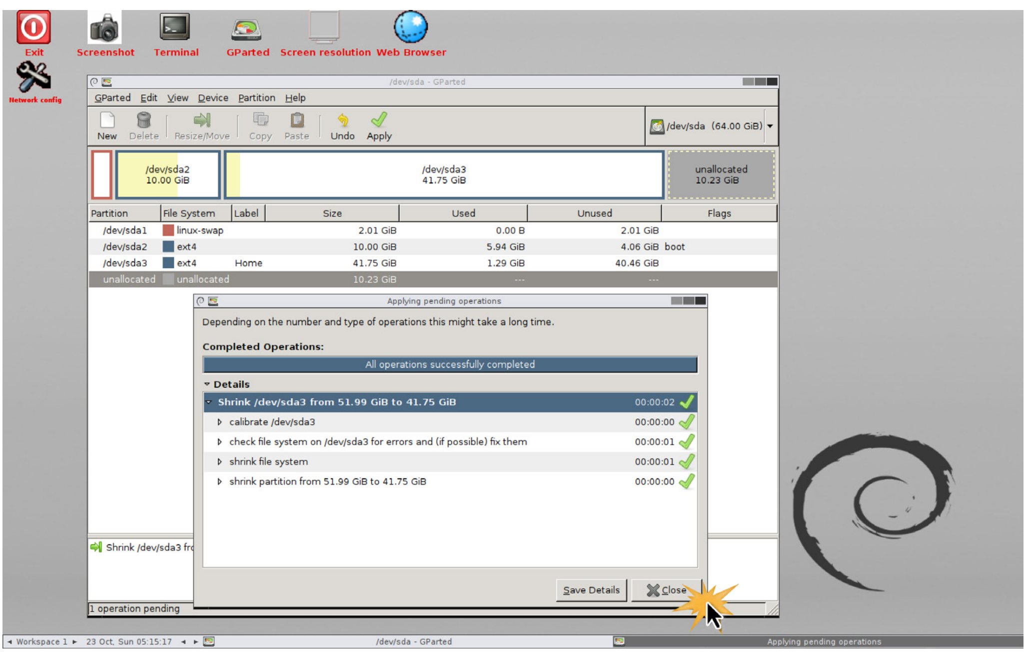
Αλλάζουμε το μέγεθος της κατάτμησης είτε σύροντας τη μπάρα της από αριστερά ή από δεξιά, είτε πληκτρολογώντας τις κατάλληλες αριθμητικές τιμές στα σχετικά πεδία. Αφού ικανοποιηθούμε με τις αλλαγές μας κάνουμε κι ένα κλικ στο κουμπί Resize/Move, κάτω δεξιά.



*Ιδού ο ελεύθερος χώρος που δημιουργήθηκε με βάση τις αλλαγές που μόλις κάναμε. Προσέξτε: Οι αλλαγές *δεν* πρόκειται να εφαρμοστούν αν δεν πατήσουμε πάνω στο κουμπάκι Apply.*



Τελευταία ευκαιρία για ν' αλλάξουμε γνώμη και να μη φέρουμε τα πάνω κάτω στο σύμπαν μας! Αν και η αλλαγή μεγέθους της κατάτμησης που πρόκειται να κάνουμε είναι μη-καταστροφική διαδικασία, μ' άλλα λόγια δεν πρόκειται να χαθούν τα δεδομένα που υπάρχουν στο partition, το GParted για άλλη μια φορά ζητά την άδειά μας για τη συνέχεια.



Τέλεια όλα! Το GParted μόλις άλλαξε το μέγεθος της κατάτμησης που του υποδείξαμε, ενώ εμείς έχουνε τώρα 10GB αποθηκευτικού χώρου τα οποία ελεύθερα μπορούμε να κατανείμουμε σε κάποιο άλλο partition.

Skill: Beginner
Tags: Raspberry Pi, Raspbian

Το Raspbian στο Raspberry Pi

Λίγο καιρό πριν εκδηλώθηκε για άλλη μια φορά η αγάπη μας προς το Raspberry, οπότε κι αγοράσαμε ένα πακέτο με το Pi 3 model B. Στην κάρτα Micro SD που το συνόδευε υπήρχε το NOOBS και πρώτη μας δουλειά ήταν να το αντικαταστήσουμε μ' ένα image του Raspbian.

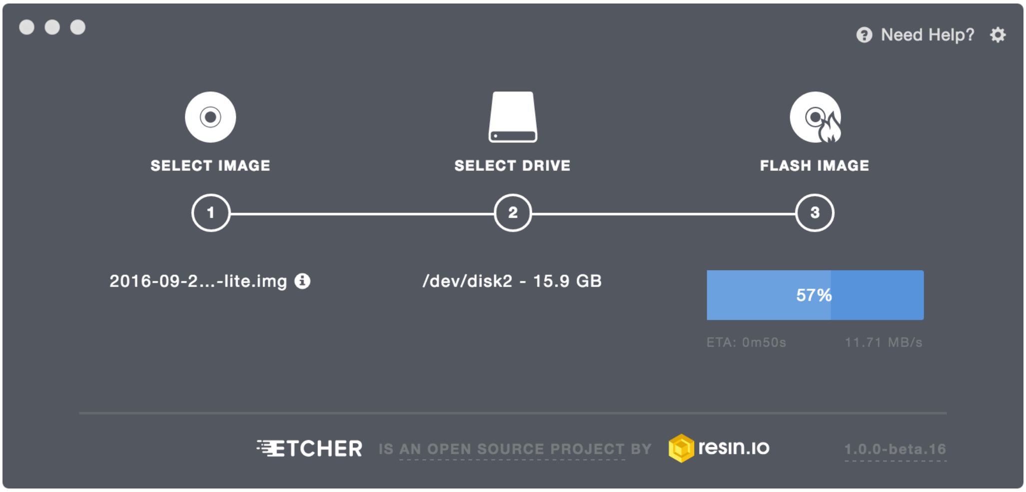
Το πακέτο το βρήκαμε στο γερμανικό Amazon (https://www.amazon.de/gp/product/B01DC6MKAQ) και περιλαμβάνει ό,τι χρειάζεται κάποιος που προορίζει το Raspberry Pi (https://www.raspberrypi.org) για χρήση server, συνεπώς δεν έχει ανάγκη για οθόνη, πληκτρολόγιο ή ποντίκι. Όπως ήδη αναφέραμε, στην κάρτα Micro SD υπήρχε το NOOBS (New Out Of Box Software, https://github.com/raspberrypi/noobs). Ο εν λόγω installer απαιτεί οθόνη και πληκτρολόγιο, ίσως και ποντίκι. Για να είμαστε ειλικρινείς, κατά την αγορά δεν είχαμε δώσει καμία σημασία στο περιεχόμενο της Micro SD. Λίγες μέρες αργότερα, όταν ξεκινήσαμε για πρώτη φορά το Raspberry Pi και δεν μπορούσαμε να κάνουμε SSH login από ένα MacBook, αμέσως πήραμε το καλώδιο HDMI που υπάρχει στο πακέτο και συνδέσαμε τη συσκευή στην τηλεόραση. Είδαμε τότε το αρχικό μενού του NOOBS, από το οποίο επιλέγουμε λειτουργικό σύστημα προς εγκατάσταση. Θέλαμε το Raspbian (http://raspbian.org) και κάλλιστα θα μπορούσαμε να το εγκαταστήσουμε με τη βοήθεια του NOOBS. Αντί όμως να ψάξουμε για πληκτρολόγιο και ποντίκι κλείσαμε το Pi, βάλαμε την κάρτα Micro SD στον SanDisk adapter που επίσης περιλαμβάνεται στο πακέτο, τον συνδέσαμε στη θύρα SD του laptop και φροντίσαμε για τα περαιτέρω.

Στο άρθρο που τώρα διαβάζετε συζητάμε για το πώς περνάμε manually το Raspbian στο Raspberry Pi 3, βεβαίως και για το πώς ρυθμίζουμε το λειτουργικό ώστε να συμπεριφέρεται όπως ακριβώς θέλουμε και να είναι σαφώς ασφαλέστερο. Σε επόμενα άρθρα θα δείξουμε, αναλυτικά και βήμα προς βήμα, μερικά ενδιαφέροντα πρότζεκτ που έχουμε κατά νου και τα υλοποιούμε γύρω από το Raspberry Pi. Στο πρώτο απ' αυτά τα άρθρα θα ασχοληθούμε με το NextCloud, τον πολλά υποσχόμενο διάδοχο του πάλαι ποτέ ownCloud. Αλλά ας πάρουμε τα πράγματα από την αρχή.

Λήψη Raspbian και μεταφορά στη Micro SD

Ένα image του συγκεκριμένου λειτουργικού συστήματος μπορούμε να κατεβάσουμε από το https://www.raspberrypi.org/downloads/raspbian. Θα γνωρίζετε βεβαίως ότι το Raspbian βασίζεται στο Debian, ίσως και ότι για download διατίθενται δύο εκδοχές: η PIXEL και η LITE. Η πρώτη προορίζεται για χρήση desktop και η δεύτερη κυρίως για server. Επιλέγοντας την εκδοχή LITE μετά από λίγο έχουμε στο

δίσκο μας το αρχείο 2016-09-23-raspbian-jessie-lite.zip – ή τουλάχιστον αυτό κατεβάσαμε εμείς την ημέρα του download. Αφού το αποσυμπιέσουμε παίρνουμε το 2016-09-23-raspbian-jessie-lite.img: πρόκειται για το image file που γράφουμε πάνω στη Micro SD. Ένα βολικό κι αξιόπιστο εργαλείο για τη διαδικασία της εγγραφής είναι το Etcher, το οποίο διατίθεται δωρεάν από το https://etcher.io (υπάρχουν εκδοχές για Linux, macOS και Windows). Το εργαλείο είναι απλούστατο στη χρήση και δεν υπάρχει κάποιο σχόλιο που αξίζει να κάνουμε.



Το Etcher είναι ένα άριστο εργαλείο για τη σωστή εγγραφή images σε κάρτες SD και USB flash drives. Διατίθεται για Linux, macOS και Windows. Στο στιγμιότυπο το βλέπουμε να γράφει το image του Raspbian στη συσκευή /dev/disk2 (η Micro SD).

Προσοχή, προσοχή, προσοχή!

Τη στιγμή που διαβάζετε το παρόν είναι πιθανό να έχετε ήδη κατεβάσει τη νεότερη έκδοση του Raspbian, η οποία σε σχέση μ' αυτή που χρησιμοποιήσαμε για τις ανάγκες του άρθρου εισάγει μια σειρά από βελτιώσεις ασφαλείας. Στο πλαίσιο αυτών, ο OpenSSH server είναι απενεργοποιημένος. Το γεγονός μάλλον περνά απαρατήρητο απ' όσους έχουν την εκδοχή PIXEL. Εκείνοι όμως που έχουν την εκδοχή LITE και το Raspberry Pi τους είναι (σκοπίμως) headless, προς μεγάλη τους απογοήτευση θα διαπιστώσουν ότι δεν μπορούν να κάνουν SSH login στο σύστημα. Η λύση είναι να δημιουργήσουμε ένα αρχείο με όνομα "ssh" (χωρίς τα εισαγωγικά), κάτω από τον κατάλογο /boot. Ο εν λόγω κατάλογος αποτελεί το mount point της ομώνυμης κατάτμησης που είναι διαμορφωμένη κατά vfat. Έτσι, η δημιουργία του αρχείου γίνεται πανεύκολα ανεξαρτήτως του λειτουργικού που τρέχει ο υπολογιστής μας. Στην επόμενη εκκίνηση του Raspbian το αρχείο ssh θα εντοπιστεί κι αυτό θα σηματοδοτήσει την ενεργοποίηση αλλά και την εκκίνηση του OpenSSH server, όπως επίσης και τη διαγραφή του προαναφερθένος αρχείου. Κι ένα τελευταίο σχόλιο: Αν στην προηγούμενη πρόταση εντοπίσατε έναν πλεονασμό (ενεργοποίηση κι εκκίνηση), είναι που δεν έχετε ακόμη διαβάσει το άρθρο μας περί Systemd (https://deltahacker.gr/?p=16816).

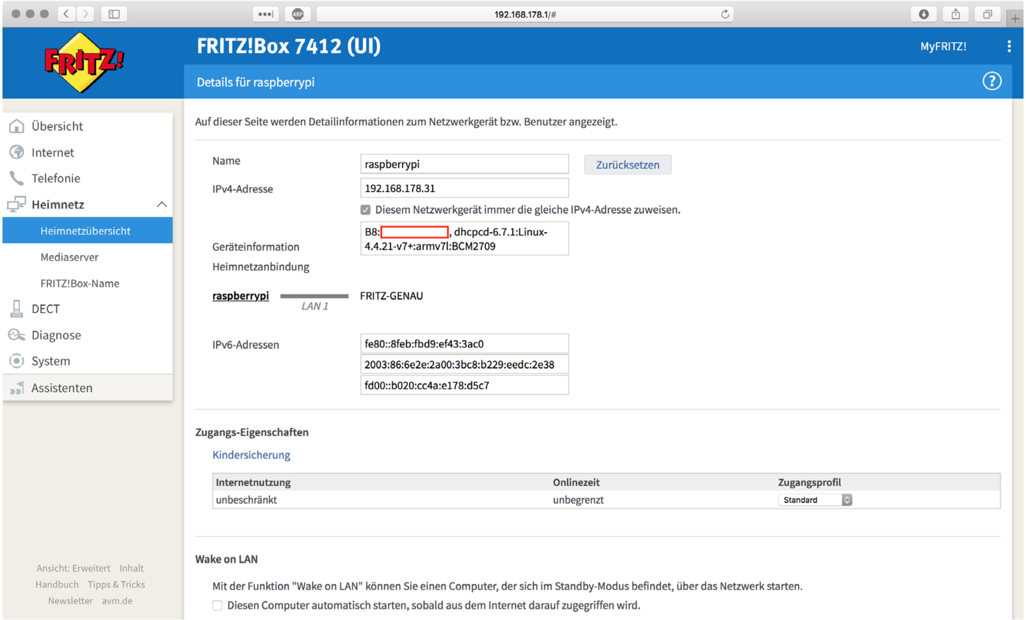
Εκκίνηση του Raspberry και πρώτη σύνδεση μέσω SSH

Αφού βάλουμε τη Micro SD με το Raspbian στο Raspberry Pi (στο εξής RasPi), συνδέσουμε τη συσκευή με ένα καλώδιο Ethernet στον router και βεβαίως στο ρεύμα, λίγα δευτερόλεπτα αργότερα θα μπορούμε να κάνουμε login μέσω SSH. Ποιο είναι όμως το IP του RasPi μας; Ένας τρόπος για να το βρούμε είναι σαρώνοντας το τοπικό δίκτυο, π.χ., με τη βοήθεια του nmap. Εναλλακτικά, κοιτάζουμε στο web panel του router και ψάχνουμε για τη νέα συσκευή. Δείτε τα δύο screenshots που ακολουθούν, διαβάστε τις αντίστοιχες περιγραφές.

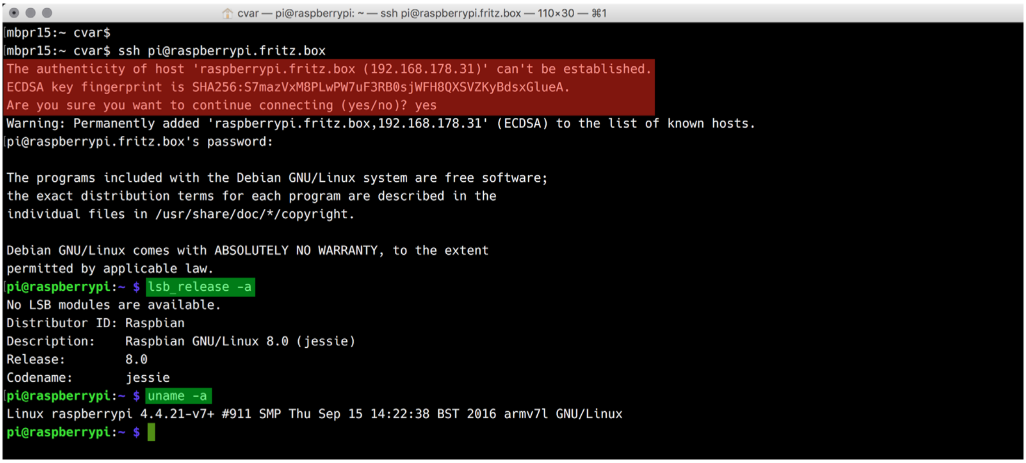
```
~ — ttys000
mbpr15:~ cvar$
mbpr15:~ cvar$ nmap -sn 192.168.178.*

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-26 09:53 CET
Nmap scan report for fritz.box (192.168.178.1)
Host is up (0.0076s latency).
Nmap scan report for keflavik-wifi.fritz.box (192.168.178.22)
Host is up (0.0058s latency).
Nmap scan report for mbpr15.fritz.box (192.168.178.25)
Host is up (0.00016s latency).
Nmap scan report for android-89c1b6b0293cef6f.fritz.box (192.168.178.27)
Host is up (0.031s latency).
Nmap scan report for kindle-2ba20c126.fritz.box (192.168.178.29)
Host is up (0.0068s latency).
Nmap scan report for raspberrypi.fritz.box (192.168.178.31)
Host is up (0.0070s latency).
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.94 seconds
mbpr15:~ cvar$
```

Σάρωση του τοπικού δικτύου με χρήση του nmap. Η παράμετρος -sn εκτελεί ένα απλό ping scan, το οποίο για την περίπτωσή μας είναι ακριβώς ό,τι χρειάζεται. Όπως βλέπετε, η τελευταία συσκευή που βρέθηκε είναι το RasPi μας (το hostname του Raspbian είναι χαρακτηριστικό).



Ιδού το RasPi μέσα από το web panel του τοπικού router. Διαφορετικοί routers είναι πιθανό να έχουν εντελώς διαφορετικά web panels. Ψάξτε για τη σελίδα όπου παρατίθενται όλες οι συσκευές του τοπικού δικτύου. Χάρη στο hostname που στέλνει το Raspbian στον όποιο διαθέσιμο DHCP server, δεν θα δυσκολευτείτε να εντοπίσετε τη συσκευή.



Την πρώτη φορά που επιχειρούμε σύνδεση μέσω SSH μάς ζητείται επιβεβαίωση για το fingerprint του RasPi. Μάλλον το απομακρυσμένο host δεν ανήκει σε κάποιον MiTM attacker, οπότε χωρίς άγχος δεχόμαστε την εγκυρότητα του fingerprint και προχωράμε :)

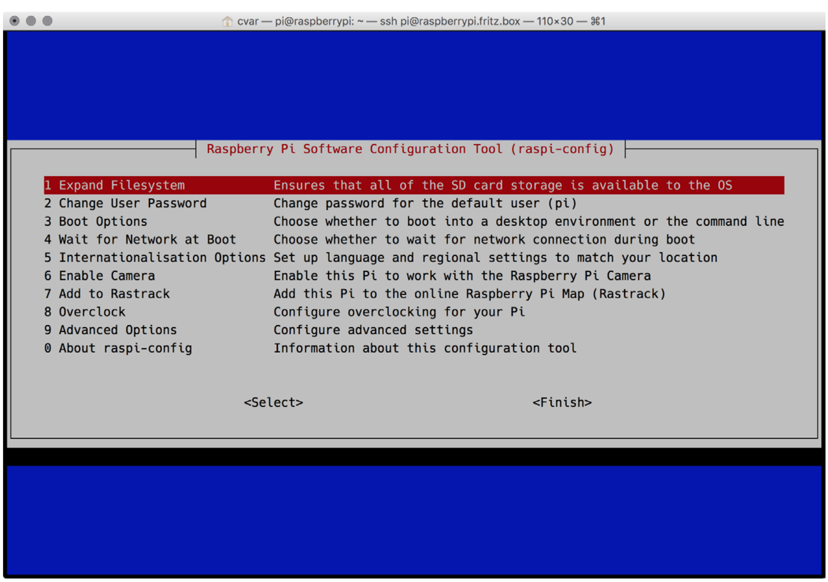
Αφού βρούμε τη διεύθυνση IP του RasPi, με τη βοήθεια του αγαπημένου μας SSH client θα συνδεθούμε στο λογαριασμό του Raspbian με username το pi και password το raspberry.

Τα απαραίτητα περί ασφάλειας

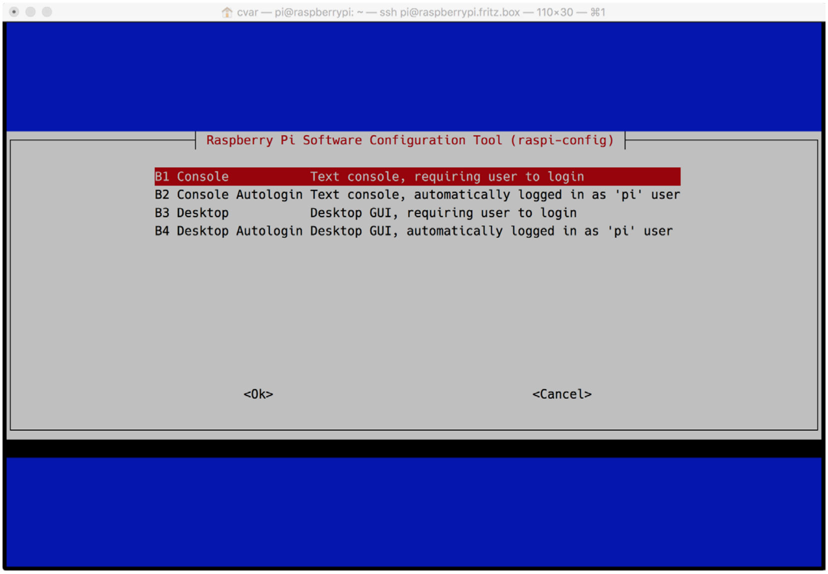
Προτείνεται τώρα ν' αλλάξουμε το προκαθορισμένο password του χρήστη pi. Προς τούτο, αρκεί να τρέξουμε το εργαλείο passwd. Θα μας ζητηθεί το τρέχον password του pi, το οποίο όπως αναφέραμε είναι raspberry. Ακολούθως θα πληκτρολογήσουμε το νέο password – δύο φορές, για λόγους ασφαλείας. Και μετά απ' αυτό, καλό θα ήταν να ρυθμίσουμε έτσι τον OpenSSH server του pi ώστε να δέχεται authentication *μόνο* με βάση τα κλειδιά SSH. Στο όλο θέμα έχουμε αναφερθεί και γράψει πολλές φορές. Αν όμως είναι η πρώτη φορά που διαβάζετε κάτι σχετικό, τότε: α) δείτε το αναλυτικό άρθρο στο https://deltahacker.gr/?p=13357, β) καλώς ήλθατε στο περιοδικό.

Βασικές ρυθμίσεις συστήματος

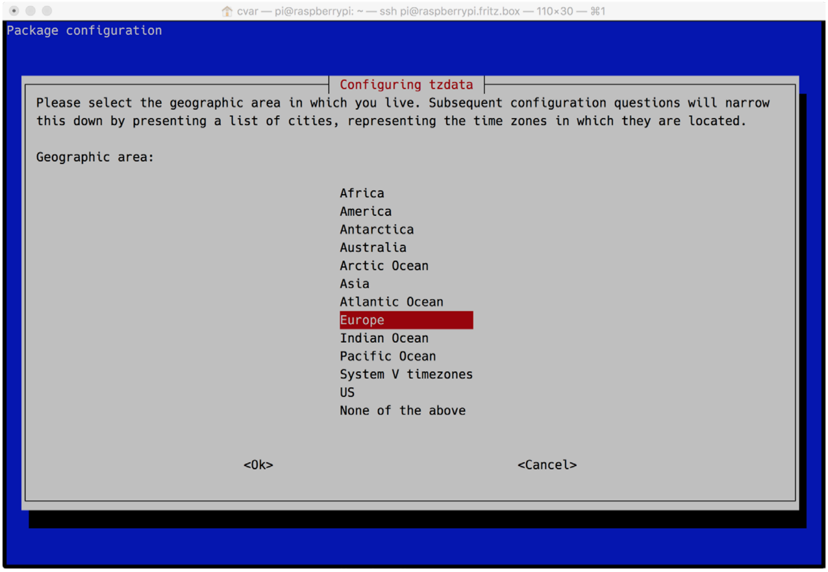
Για τη ρύθμιση του Raspbian υπάρχει το βολικό εργαλείο raspi-config, το οποίο λειτουργεί στην κονσόλα απλού κειμένου και το τρέχουμε με δικαιώματα διαχειριστή συστήματος. Μόλις αρχίσαμε να παίζουμε με το Raspbian, οπότε καλό είναι να εξερευνήσουμε και το σύστημα μενού του raspi-config. Δείτε μερικά χαρακτηριστικά screenshots.



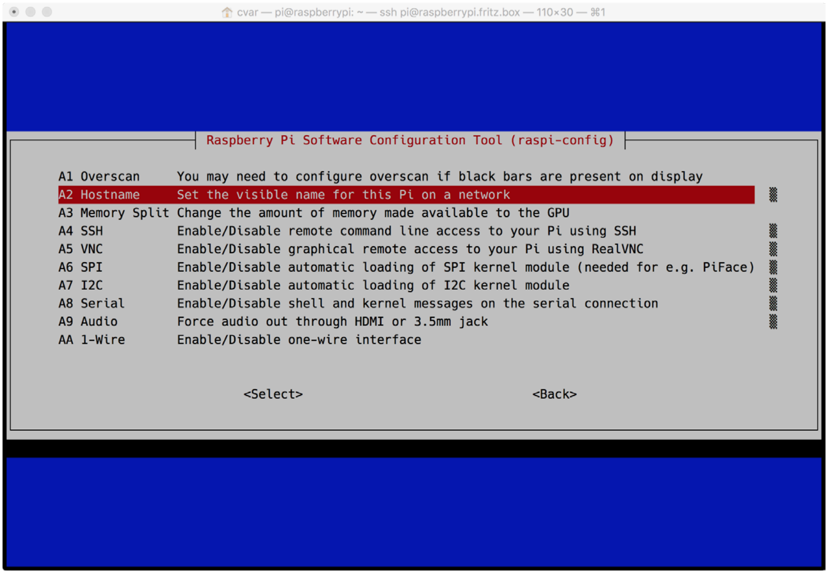
Μετά την πρώτη μας σύνδεση στον προκαθορισμένο λογαριασμό χρήστη του Raspbian, καλό θα ήταν να τρέξουμε και το εργαλείο raspi-config (λειτουργεί στο περιβάλλον του τερματικού).



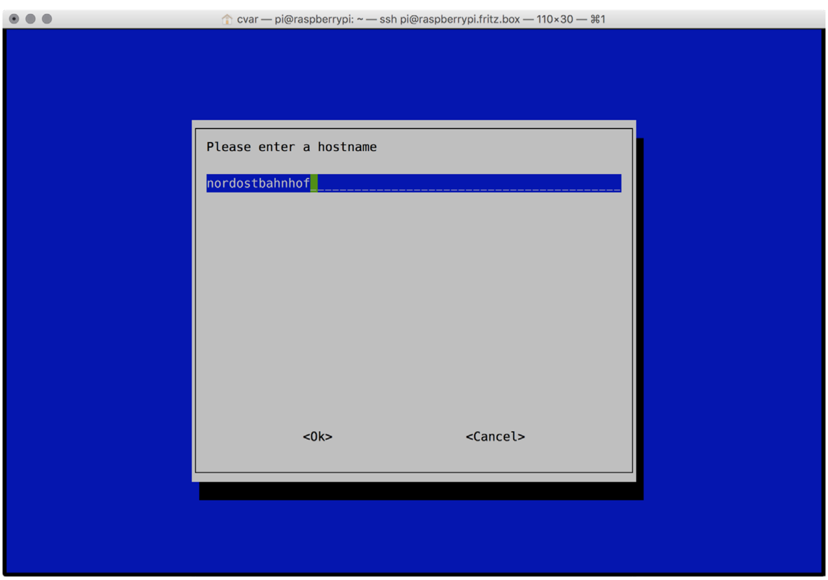
Σε τι περιβάλλον θέλουμε να ξεκινά το Raspbian; Για τη χρήση που προορίζουμε το δικό μας δεν θέλουμε το περιβάλλον γραφικών, αλλά εκείνο της κονσόλας απλού κειμένου. Επίσης, δεν επιθυμούμε αυτόματη σύνδεση στο λογαριασμό του χρήστη μας. Κάτι τέτοιο θα ήταν επιθυμητό σε άλλα σενάρια, όπου ο κάτοχος του RasPi το έχει κυρίως για χρήση desktop και δεν υπάρχει κάποιος άλλος ο οποίος θα χρησιμοποιούσε τη συσκευή χωρίς να έχει σχετική άδεια.



Κάτι που ορισμένοι (ονόματα δεν λέμε) ξεχνούν να κάνουν για το RasPi τους, είναι να καθορίζουν τη σωστή ζώνης ώρας. Η σχετική επιλογή στο σύστημα μενού του raspi-config μάς υπενθυμίζει αυτή την παράλειψη.



Μια από τις ρυθμίσεις που, για εμάς τουλάχιστον, είναι απαραίτητη, αφορά στον καθορισμό hostname για το λειτουργικό. Από προεπιλογή, το hostname είναι raspberrypi.



Ιδού το νέο hostname του Raspbian. Ναι, το edition name του τεύχους 056 επιμένει :D

Σημείωση για τα locales

Στο raspi-config θα παρατηρήσετε ότι υπάρχει επιλογή για τον καθορισμό των locales. Αν και κάναμε τις επιλογές μας, λίγο αργότερα στο τερματικό παίρναμε προειδοποιήσεις περί "κενών" μεταβλητών locales (π.χ., τέτοια μηνύματα είχαμε κατά τη διάρκεια εγκαταστάσεων/αναβαθμίσεων πακέτων). Αν θέλετε να είστε βέβαιος ότι τα locales έχουν τεθεί σωστά, με δικαιώματα διαχειριστή κάντε τις επεμβάσεις σας στο αρχείο /etc/default/locale και κατόπιν δώστε `sudo locale-gen`. Καλού κακού, κάντε και μια επανεκκίνηση με ένα `sudo reboot`. Δείτε, παρεμπιπτόντως, τα περιεχόμενα του /etc/default/locale στο δικό μας RasPi:

```
pi@nordostbahnhof:~ $ cat /etc/default/locale
#  File generated by update-locale
LANG=en_US.UTF-8
LC_ALL=en_US.UTF-8
LC_CTYPE=en_US.UTF-8
LANGUAGE=en_US.UTF-8
```

Αναβάθμιση και προσωρινός επίλογος

Στο σημείο αυτό το Raspbian είναι σχεδόν έτοιμο για οποιονδήποτε ρόλο σκοπεύουμε να του δώσουμε. Το μόνο που μένει είναι να κάνουμε και μια αναβάθμιση. Όπως στο Debian, στο Ubuntu, στο Mint και σε τόσες άλλες διανομές Linux που βασίζονται στο πρώτο, έτσι και στο Raspbian χρησιμοποιούμε το apt-get:

```
pi@nordostbahnhof:~ $ sudo apt-get update
pi@nordostbahnhof:~ $ sudo apt-get upgrade
```

Κατά την πρώτη αναβάθμιση που κάναμε στο Raspbian, είδαμε ότι πρόκειται ν' αναβαθμιστεί κι ο πυρήνας του λειτουργικού. Αμέσως μετά από μια τέτοια αλλαγή πρέπει ν' ακολουθεί και μια επανεκκίνηση του συστήματος — κι αν όχι "αμέσως μετά" τότε σίγουρα "το συντομότερο δυνατόν".

Σε επόμενο άρθρο δείχνουμε πώς εγκαθιστούμε και ρυθμίζουμε το NextCloud στο Raspbian (https://deltahacker.gr/?p=17061). Σκοπός μας είναι να αποκτήσουμε ένα σύστημα που έχει τη λειτουργικότητα του Dropbox και βρίσκεται αποκλειστικά υπό τον έλεγχό μας, άρα μπορούμε να του εμπιστευόμαστε την αποθήκευση των δεδομένων μας — ευαίσθητων ή όχι. Πρώτα, όμως, εγκαθιστούμε τον Apache web server και του δίνουμε δωρεάν και έγκυρο πιστοποιητικό από το Let's Encrypt. Γυρίστε τώρα στη σελίδα 88.

Skill: Intermediate
Tags: openSUSE, OS upgrade, VPS

openSUSE VPS: Μεθοδικό πέρασμα στο Leap 42.2

Η αναβάθμιση ενός συστήματος με openSUSE Leap στην αμέσως επόμενη έκδοση δύσκολα θ' αποτελούσε ευκολότερη διαδικασία. Όταν όμως μιλάμε για VPS, τότε τα πράγματα αλλάζουν. Πράγματι, όπως διαπιστώσαμε κι από τις δοκιμές μας, αν δεν έχουμε λάβει τα απαραίτητα μέτρα είναι πιθανό να καταλήξουμε ακόμη και μ' ένα λειτουργικό που δεν μπορεί καν να φορτώσει.

Περί τα μέσα του Νοεμβρίου κυκλοφόρησε το openSUSE Leap 42.2 κι αρκετοί που τρέχαμε το 42.1 αρχίσαμε τους σχεδιασμούς: αξίζει τη φασαρία η καθαρή εγκατάσταση του 42.2 ή μήπως μια αναβάθμιση στη νέα έκδοση είναι αρκετή; Αν το σκεφτούμε λίγο, γρήγορα συνειδητοποιούμε ότι κάθε προσέγγιση έχει τα θετικά και τ' αρνητικά της.

Αναλυτικότερα, με την εκ νέου εγκατάσταση βρισκόμαστε μ' ένα φρέσκο και πεντακάθαρο σύστημα. Μετά όμως ίσως δαπανήσουμε αρκετό χρόνο, προκειμένου να επαναφέρουμε το όποιο backup αλλά και για να βεβαιωθούμε ότι οι επιλογές και οι προτιμήσεις μας ισχύουν *και* στο καινούργιο περιβάλλον.

Αν πάλι ακολουθήσουμε την οδό της αναβάθμισης διασφαλίζουμε ότι το ανανεωμένο σύστημα, καθώς και οι εγκατεστημένες υπηρεσίες κι εφαρμογές, συνεχίζουν να συμπεριφέρονται σύμφωνα με τις προσαρμογές που είχαμε κάνει. Αλλά το θέμα είναι ότι με την αναβάθμιση ποτέ δεν μπορούμε να είμαστε 100% βέβαιοι για τα (περιττά) μπαγκάζια που ενδεχομένως θα κληρονομήσει η νέα έκδοση από την παλιά.

Υπάρχει και μια ενδιάμεση προσέγγιση, την οποία προτείνεται ν' ακολουθούμε ειδικά αν στο σύστημά μας το /home είναι προσαρτημένο σε ξεχωριστή κατάτμηση. Πιο συγκεκριμένα, λέμε στον installer του openSUSE ότι θέλουμε να διαμορφώσει (format) όλα τα διαμερίσματα, εκτός από εκείνο του /home. Πραγματοποιούμε μ' αυτό τον τρόπο μια καθαρότατη εγκατάσταση, αλλά επειδή τα αρχεία ρυθμίσεων του χρήστη ή των χρηστών είναι κάτω από το /home βεβαιωνόμαστε ότι οι εφαρμογές θα είναι ρυθμισμένες όπως ακριβώς θέλουμε. Βεβαίως, τα αρχεία ρυθμίσεων των υπηρεσιών, που βρίσκονται κάτω από το /etc, θα τα επαναφέρουμε από το backup μας.

Σημείωση. Σε κάθε περίπτωση, είναι νομίζουμε προφανές ότι πριν την εγκατάσταση ή την αναβάθμιση οφείλουμε να έχουμε φροντίσει για ένα καλό backup. Αν μάλιστα μιλάμε για VM ή για VPS, τότε και η λήψη ενός επίκαιρου snapshot προτείνεται ενθουσιωδώς.

Ορμώμενοι από πρόσφατη περιπέτεια που είχαμε μ' ένα VPS στη Hetzner (https://deltahacker.gr/?p=16962), δείχνουμε στη συνέχεια τη διαδικασία αναβάθμισης από το openSUSE Leap 42.1 στο 42.2. Θα εργαστούμε από τη γραμμή εντολών του λειτουργικού κι όχι μέσα από το περιβάλλον (γραφικών) του YaST. Παρεμπιπτόντως, αναλόγως του VPS provider ίσως έχουμε δυνατότητα *μόνο* για την πρώτη προσέγγιση, δηλαδή για αναβάθμιση από τη γραμμή εντολών.

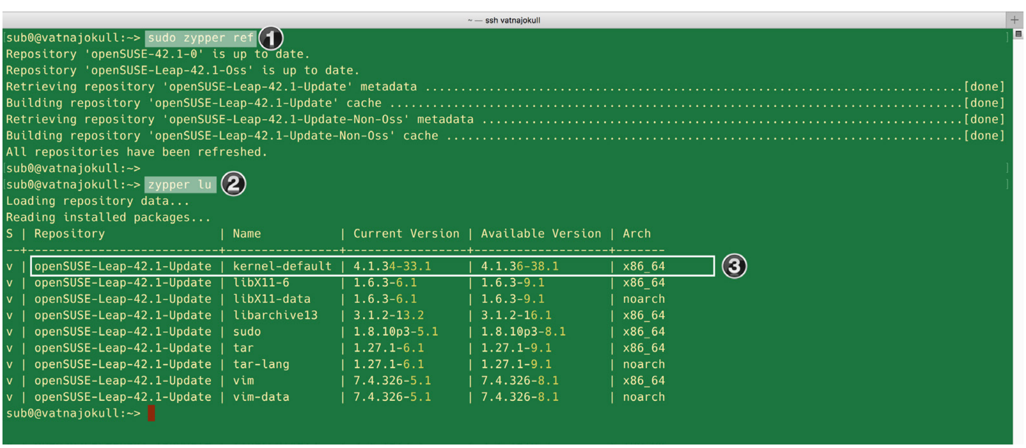
Σημείωση. Αν κι απευθυνόμαστε κυρίως σε κατόχους VPS με openSUSE Leap 42.1, η διαδικασία που παρουσιάζουμε εφαρμόζεται παρόμοια και σε τυπικά PCs ή VMs — πάντα με openSUSE. Ας τονιστεί εξάλλου ότι η συγκεκριμένη μέθοδος αναβάθμισης δουλεύει χωρίς προβλήματα μόνον όταν *δεν* παρεμβάλλεται κάποια έκδοση μεταξύ αυτής που τώρα βρισκόμαστε κι εκείνης που θέλουμε να φτάσουμε.

Προετοιμασία VPS και μια τρύπα στο νερό

Συνδεόμαστε στον απομακρυσμένο host με το openSUSE Leap 42.1 και φροντίζουμε ώστε το λειτουργικό να είναι ενημερωμένο. Αρχικά πληκτρολογούμε:

```
sub0@vatnajokull:~> sudo zypper ref
sub0@vatnajokull:~> zypper lu
```

Μεταξύ των διαθέσιμων updates για το openSUSE του VPS μας, συμπεριλαμβανόταν και νέα έκδοση του πυρήνα.



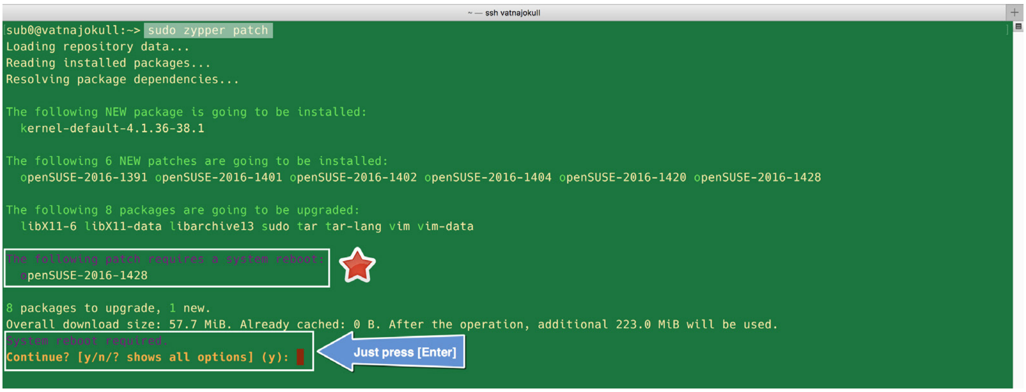
```
sub0@vatnajokull:~> sudo zypper ref
Repository 'openSUSE-42.1-0' is up to date.
Repository 'openSUSE-Leap-42.1-Oss' is up to date.
Retrieving repository 'openSUSE-Leap-42.1-Update' metadata ..........................[done]
Building repository 'openSUSE-Leap-42.1-Update' cache ...............................[done]
Retrieving repository 'openSUSE-Leap-42.1-Update-Non-Oss' metadata ..................[done]
Building repository 'openSUSE-Leap-42.1-Update-Non-Oss' cache .......................[done]
All repositories have been refreshed.
sub0@vatnajokull:~>
sub0@vatnajokull:~> zypper lu
Loading repository data...
Reading installed packages...
S | Repository                 | Name           | Current Version | Available Version | Arch
--+----------------------------+----------------+-----------------+-------------------+-------
v | openSUSE-Leap-42.1-Update | kernel-default | 4.1.34-33.1     | 4.1.36-38.1       | x86_64
v | openSUSE-Leap-42.1-Update | libX11-6       | 1.6.3-6.1       | 1.6.3-9.1         | x86_64
v | openSUSE-Leap-42.1-Update | libX11-data    | 1.6.3-6.1       | 1.6.3-9.1         | noarch
v | openSUSE-Leap-42.1-Update | libarchive13   | 3.1.2-13.2      | 3.1.2-16.1        | x86_64
v | openSUSE-Leap-42.1-Update | sudo           | 1.8.10p3-5.1    | 1.8.10p3-8.1      | x86_64
v | openSUSE-Leap-42.1-Update | tar            | 1.27.1-6.1      | 1.27.1-9.1        | x86_64
v | openSUSE-Leap-42.1-Update | tar-lang       | 1.27.1-6.1      | 1.27.1-9.1        | noarch
v | openSUSE-Leap-42.1-Update | vim            | 7.4.326-5.1     | 7.4.326-8.1       | x86_64
v | openSUSE-Leap-42.1-Update | vim-data       | 7.4.326-5.1     | 7.4.326-8.1       | noarch
sub0@vatnajokull:~>
```

Φρεσκάρισμα των αποθετηρίων του openSUSE Leap 42.1 (1) και προβολή των πακέτων για τα οποία υπάρχει νεότερη έκδοση (2). Μεταξύ αυτών συμπεριλαμβάνεται και το πακέτο με τον πυρήνα του συστήματος (3).

Η αναβάθμιση των πακέτων ξεκινά με ένα

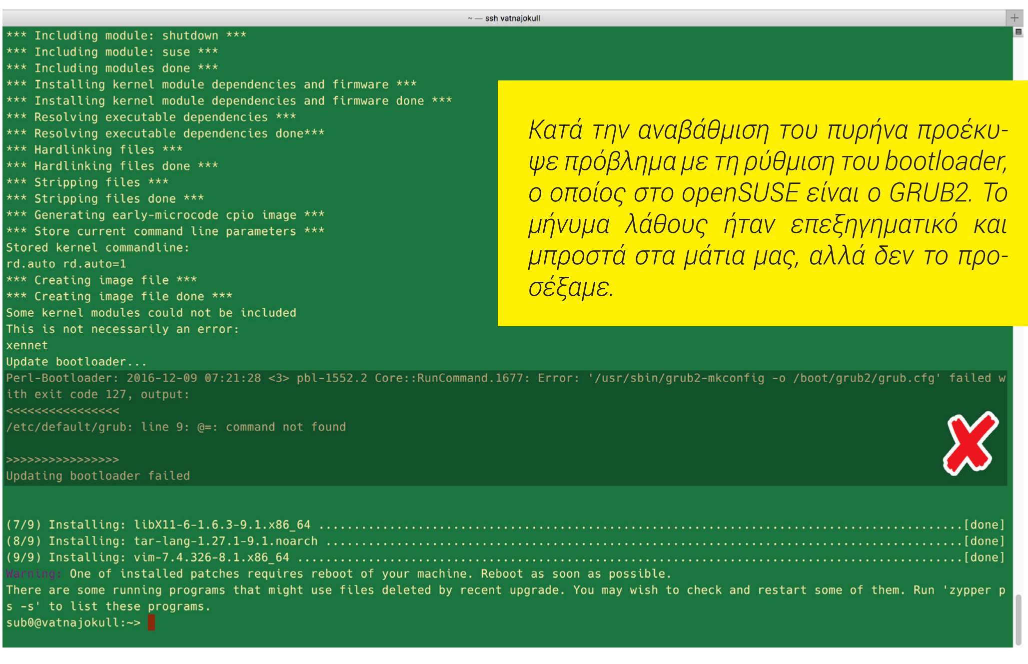
```
sub0@vatnajokull:~> sudo zypper patch
```

Γενικά, όταν έχουμε αναβάθμιση του πυρήνα τότε αμέσως μετά χρωστάμε κι ένα reboot.



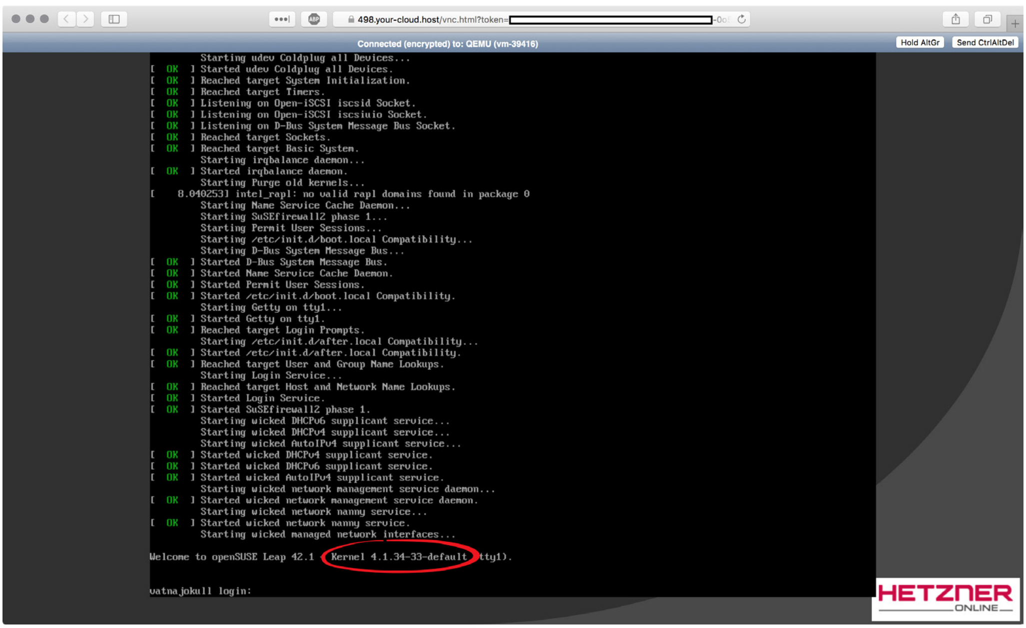
Μετά την αναβάθμιση του πυρήνα οφείλουμε να επανεκκινούμε το σύστημα – και μάλιστα το συντομότερο δυνατόν.

Πριν όμως το κάνουμε είναι πολύ καλή ιδέα να ρίχνουμε και μια ματιά στα μυνήματα που έχουν εμφανιστεί στο τερματικό.

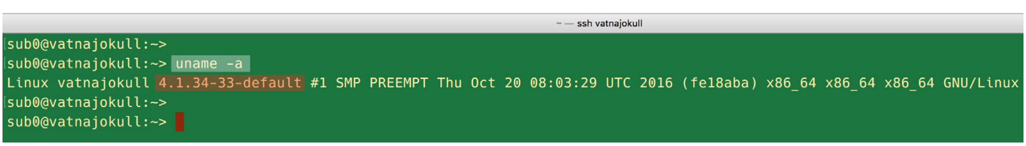


Κατά την αναβάθμιση του πυρήνα προέκυψε πρόβλημα με τη ρύθμιση του bootloader, ο οποίος στο openSUSE είναι ο GRUB2. Το μήνυμα λάθους ήταν επεξηγηματικό και μπροστά στα μάτια μας, αλλά δεν το προσέξαμε.

Στις πρώτες μας δοκιμές αποτύχαμε να δούμε το μήνυμα που υποδεικνύεται στο προηγούμενο screenshot. Η απροσεξία μας ενδεχομένως να οφειλόταν στο γεγονός ότι κάθε λίγο και λιγάκι αναβαθμίζουμε τον πυρήνα κι όλα πηγαίνουν μια χαρά, ίσως όμως απλά να έφταιγε η αφηρημάδα μας και η προηγούμενη πρόταση να είναι μια μέτρια δικαιολογία. Τελικά, με τη συγκεκριμένη αναβάθμιση του πυρήνα κάναμε μια τρύπα στο νερό. Δείτε τα ακόλουθα δύο screenshots, διαβάστε και τις αντίστοιχες περιγραφές.

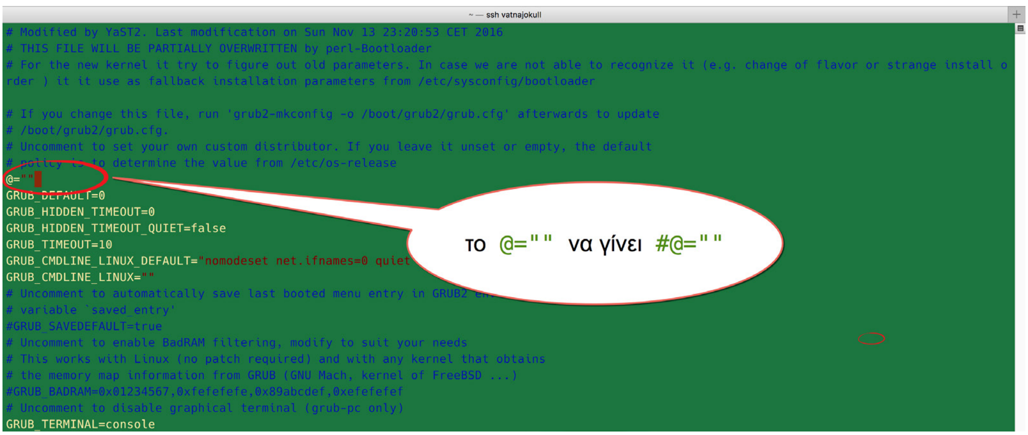


Μετά το reboot απλά χαζεύαμε τα μηνύματα της διαδικασίας επανεκκίνησης στη web VNC console που προσφέρει ο VPS provider. Παρατηρήστε την έκδοση του πυρήνα στο μήνυμα καλωσορίσματος, ακριβώς πάνω από το login prompt: είναι η 4.1.34-33. Μάλιστα. Πιθανώς δεν θα θυμόσαστε ποια είναι η νέα έκδοση του πυρήνα που θα έπρεπε να έχουμε, έτσι δεν είναι; Βρείτε τη στα προηγούμενα screenshots. Αλλά γιατί να σας παιδεύουμε; Σας λέμε από εδώ ότι είναι η 4.1.36-38. Αντί λοιπόν για τη νέα έκδοση του πυρήνα είχαμε ακόμη την παλιά – ή τουλάχιστον αυτό φανέρωνε το μήνυμα στην κονσόλα. Μήπως όμως επρόκειτο για λάθος μήνυμα; Θα έπρεπε να συνδεθούμε στο λογαριασμό του χρήστη μας και να ελέγξουμε.

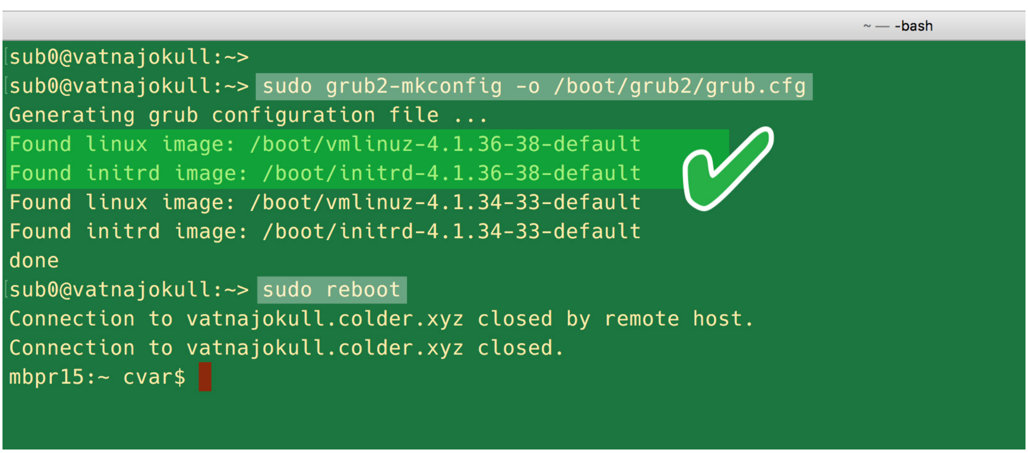


Συνδεθήκαμε (μέσω SSH) στο λογαριασμό του χρήστη μας στο VPS και πληκτρολογήσαμε `uname -a`*. Όχι. Δεν είχαμε το νέο πυρήνα. Η διαδικασία της αναβάθμισής είχε αποτύχει. Ή μπορεί και να είχε πετύχει, αλλά ο bootloader εξακολουθούσε να φορτώνει τον προηγούμενο πυρήνα. Όπως και να 'χε, τον καινούργιο πυρήνα δεν τον χρησιμοποιούσαμε.*

Από το μήνυμα λάθους που αρχικά αποτύχαμε να προσέξουμε, φαινόταν ότι το πρόβλημα δεν αφορούσε στην ίδια την εγκατάσταση του πυρήνα αλλά στη ρύθμιση του bootloader. Πιο συγκεκριμένα, το θέμα ήταν στη γραμμή 9 του αρχείου /etc/default/grub. Με δικαιώματα root ανοίξαμε το αρχείο και "σχολιάσαμε" τη συγκεκριμένη γραμμή. Σε άλλες πέντε εγκαταστάσεις του openSUSE που συντηρούμε, η γραμμή αυτή δεν υπάρχει στο /etc/default/grub. Η παρουσία της στο VPS μάς κάνει να πιστεύουμε ότι οφείλεται σε misconfiguration, π.χ., λόγω κάποιας αλλαγής που επιχειρήσαμε να κάνουμε με το YaST κι απέτυχε να εφαρμοστεί.



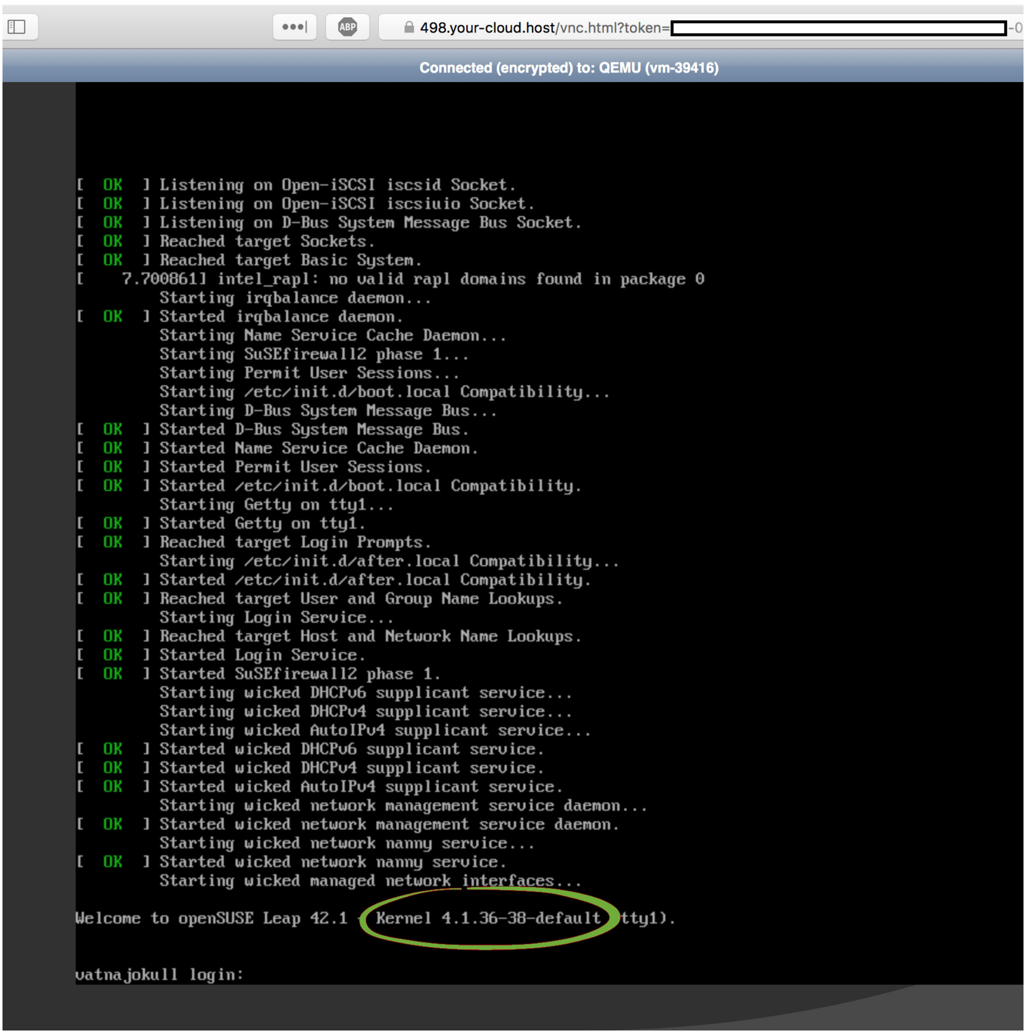
Η συγκεκριμένη γραμμή στο /etc/default/grub ήταν εκεί λόγω κάποιου misconfiguration, αντί όμως να τη διαγράψουμε σκεφτήκαμε ότι είναι ασφαλέστερο να τη "σχολιάσουμε".



Φροντίσαμε ώστε οι αλλαγές στο /etc/default/grub να ληφθούν υπόψη και, απ' ό,τι φάνηκε στα μηνύματα στο τερματικό, αυτή τη φορά ο bootloader εντόπισε τη νέα έκδοση του πυρήνα. Για να βεβαιωθούμε ότι όλα ήταν πλέον καλά, επανεκκινήσαμε το σύστημα.

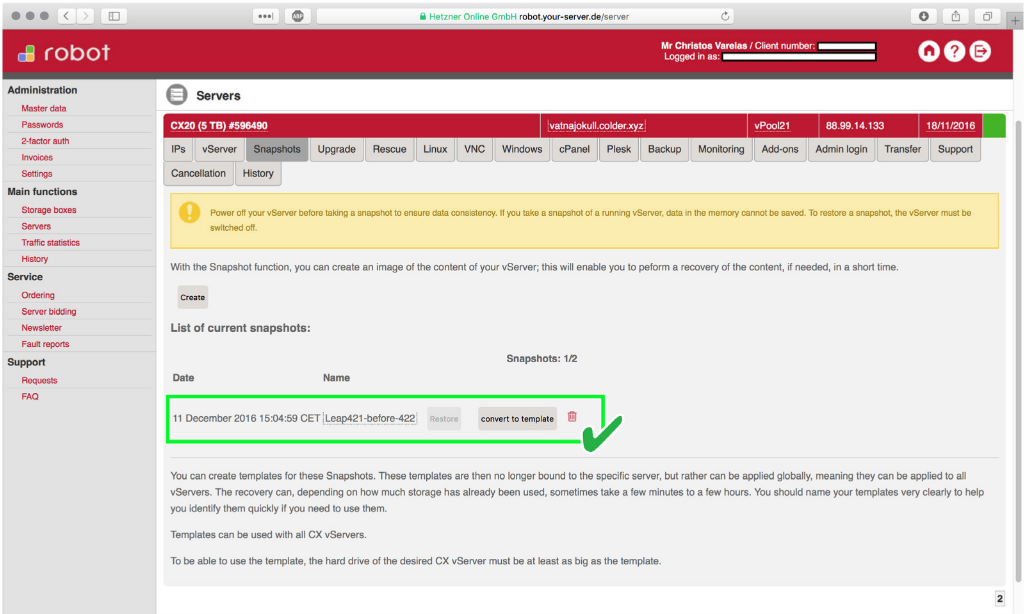
Όπως αναφέρεται στην αρχή του /etc/default/grub, μετά από κάθε αλλαγή στο αρχείο πρέπει να δίνουμε ένα `grub2-mkconfig -o /boot/grub2/grub.cfg` (με δικαιώματα root). Αμέσως μετά πληκτρολογούμε και `sudo reboot`, ώστε να βεβαιωθούμε ότι ο bootloader λειτουργεί σωστά.

Από τα μηνύματα στο τερματικό ήμασταν βέβαιοι ότι αυτή τη φορά ο bootloader είχε λάβει υπόψη την παρουσία του νέου πυρήνα. Βεβαιωθήκαμε με μια επανεκκίνηση.



Αυτή τη φορά ο GRUB2 φόρτωσε τη νεότερη έκδοση του πυρήνα. Όλα καλά!

Από τη στιγμή που έχουμε ένα πλήρως ενημερωμένο σύστημα με το openSUSE Leap 42.1, είμαστε έτοιμοι να αναβαθμιστούμε στο 42.2. Πριν προχωρήσουμε, όμως, αν ο VPS provider παρέχει δυνατότητα για snapshots τότε προτείνεται *ενθουσιωδώς* να δημιουργήσουμε ένα.



Το openSUSE Leap 42.1 στο VPS μας είναι πλήρως ενημερωμένο και είμαστε πανέτοιμοι για το άλμα προς το Leap 42.2 (no pun intended). Έχουμε πάρει και το snapshot μας, οπότε ακόμη και στην περίπτωση που επιφέρουμε το Χάος χωρίς καμία ελπίδα για μείωση της Εντροπίας, απλά θα επαναφέρουμε το snapshot και η Τάξη θα επανέλθει στον κόσμο μας.

Σημείωση. Το πόσο εμφατικά προτείνουμε τη λήψη snapshot, δύσκολα μπορούμε να σας το μεταδώσουμε. Θα σας πούμε μόνο ότι στις πρώτες μας δοκιμές, όταν το πρόβλημα με το /etc/default/grub εκδηλώθηκε στο τελευταίο στάδιο της αναβάθμισης του Leap 42.1 στο 42.2 και (φυσικά) αποτύχαμε να το προσέξουμε, το σύστημα δεν μπορούσε καν να ξεκινήσει. Αν δεν είχαμε snapshot θα μας περίμενε ένα όχι και τόσο ευχάριστο απόγευμα, ασφυκτικά γεμάτο με διαδικασίες *εκ νέου* εγκατάστασης :/

Άλμα στο 42.2 από τη γραμμή εντολών

Το σχέδιο δράσης έχει ως ακολούθως:

- **Βήμα 1.** Σημειώνουμε από πού έρχονται τα πακέτα για το OSS (Open Source Software) repository καθώς και για το repository με τις αναβαθμίσεις – πάντα του Leap 42.1.
- **Βήμα 2.** Αφαιρούμε όλα τα υπάρχοντα repositories ανεξαιρέτως.
- **Βήμα 3.** Προσθέτουμε δύο νέα repositories για τα πακέτα OSS του λειτουργικού και τις αντίστοιχες αναβαθμίσεις, τα οποία όμως αφορούν στο Leap 42.2.
- **Βήμα 4.** Φρεσκάρουμε τα νέα repositories.

- **Βήμα 5.** Αναβαθμίζουμε το λειτουργικό με βάση τα νέα repositories.
- **Βήμα 6.** Ελέγχουμε τυχόντα αρχεία ρυθμίσεων που σκοπίμως δεν τροποποιήθηκαν αλλά υπάρχει και νέα έκδοσή τους.

Βήμα 1. Ας δούμε τη λίστα με όλα τα repositories, πληκτρολογώντας `zypper lr`.

```
~ — ssh vatnajokull
sub0@vatnajokull:~>
sub0@vatnajokull:~> zypper lr
#  | Alias                     | Name                                  | Enabled | GPG Check | Refresh
---+---------------------------+---------------------------------------+---------+-----------+--------
 1 | openSUSE-42.1-0           | openSUSE-42.1-0                       | Yes     | (r ) Yes  | Yes
 2 | repo-debug                | openSUSE-Leap-42.1-Debug              | No      | ----      | Yes
 3 | repo-debug-non-oss        | openSUSE-Leap-42.1-Debug-Non-Oss      | No      | ----      | Yes
 4 | repo-debug-update         | openSUSE-Leap-42.1-Update-Debug       | No      | ----      | Yes
 5 | repo-debug-update-non-oss | openSUSE-Leap-42.1-Update-Debug-Non-Oss | No    | ----      | Yes
 6 | repo-non-oss              | openSUSE-Leap-42.1-Non-Oss            | No      | ----      | Yes
 7 | repo-oss                  | openSUSE-Leap-42.1-Oss                | Yes     | (r ) Yes  | Yes
 8 | repo-source               | openSUSE-Leap-42.1-Source             | No      | ----      | Yes
 9 | repo-update               | openSUSE-Leap-42.1-Update             | Yes     | (r ) Yes  | Yes
10 | repo-update-non-oss       | openSUSE-Leap-42.1-Update-Non-Oss     | Yes     | (r ) Yes  | Yes
sub0@vatnajokull:~>
```

*Η λίστα με τα αποθετήρια της εγκατάστασής μας *πριν* από την αναβάθμιση. Μας ενδιαφέρουν μόνο δύο: εκείνο με τα πακέτα OSS για το openSUSE Leap 42.1, καθώς και το άλλο με τις όποιες διαθέσιμες αναβαθμίσεις.*

Τα Debug και Source repositories δεν μας ενδιαφέρουν. Από τα υπόλοιπα, εστιάζουμε την προσοχή μας στα repositories με ονόματα openSUSE-Leap-42.1-Oss και openSUSE-Leap-42.1-Update. Για καθένα εξ αυτών μπορούμε να πάρουμε περισσότερες πληροφορίες, ώστε να βρούμε τις online διευθύνσεις των πακέτων που περιλαμβάνουν. Δείτε το screenshot που ακολουθεί.

```
~ — ssh vatnajokull
sub0@vatnajokull:~> zypper lr openSUSE-Leap-42.1-Oss
Alias          : repo-oss
Name           : openSUSE-Leap-42.1-Oss
URI            : http://mirror.hetzner.de/opensuse/distribution/leap/42.1/repo/oss/
Enabled        : Yes
GPG Check      : (r ) Yes
Priority       : 99
Auto-refresh   : On
Keep Packages  : Off
Type           : yast2
GPG Key URI    :
Path Prefix    : /
Parent Service :
Keywords       :
Repo Info Path : /etc/zypp/repos.d/repo-oss.repo
MD Cache Path  : /var/cache/zypp/raw/repo-oss
sub0@vatnajokull:~>
sub0@vatnajokull:~> zypper lr openSUSE-Leap-42.1-Update
Alias          : repo-update
Name           : openSUSE-Leap-42.1-Update
URI            : http://mirror.hetzner.de/opensuse/update/leap/42.1/oss/
Enabled        : Yes
GPG Check      : (r ) Yes
Priority       : 99
Auto-refresh   : On
Keep Packages  : Off
Type           : rpm-md
GPG Key URI    :
Path Prefix    : /
Parent Service :
Keywords       :
Repo Info Path : /etc/zypp/repos.d/repo-update.repo
MD Cache Path  : /var/cache/zypp/raw/repo-update
sub0@vatnajokull:~>
```

Από πού προέρχονται τα πακέτα των δύο repositories που μας ενδιαφέρουν; Διαφορετικά: Ποιες είναι οι online διευθύνσεις των αντίστοιχων αποθετηρίων; Μπορούμε να τις μάθουμε πανεύκολα – και γρήγορα.

Ας σημειώσουμε κάπου τις ακόλουθες δύο αντιστοιχίες:

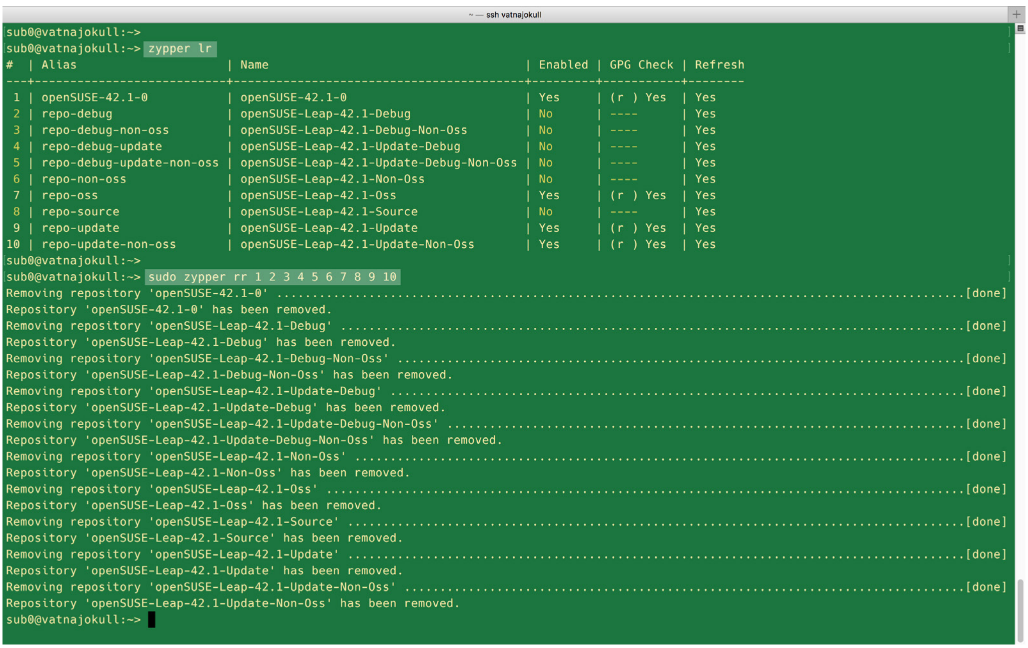
openSUSE-Leap-42.1-Oss →

http://mirror.hetzner.de/opensuse/distribution/leap/42.1/repo/oss

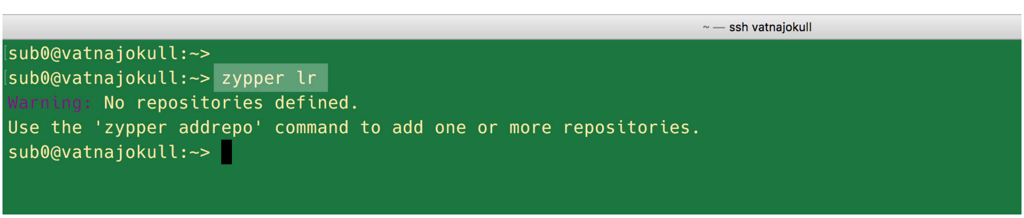
openSUSE-Leap-42.1-Update →

http://mirror.hetzner.de/opensuse/update/leap/42.1/oss

Βήμα 2. Προκειμένου να αφαιρέσουμε όλα τα υπάρχοντα repositories, αρκεί να πληκτρολογήσουμε `sudo zypper rr 1 2 3 4 5 6 7 8 9 10`.



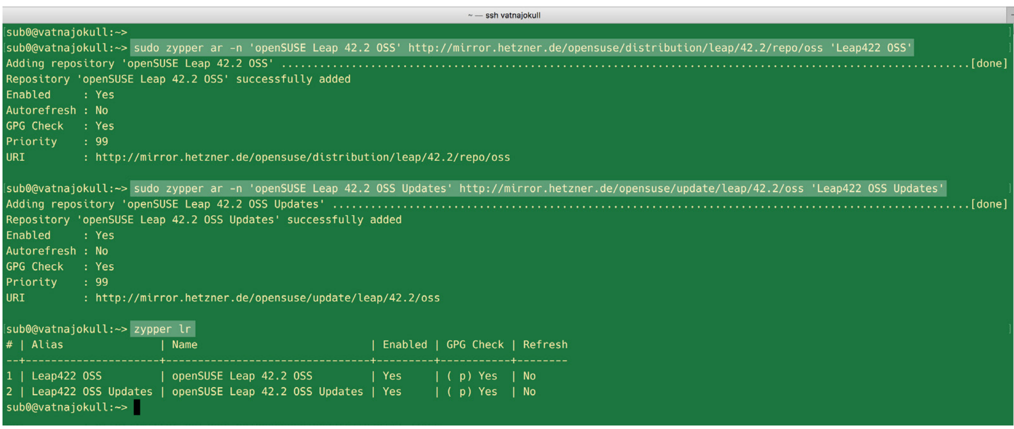
Αφαίρεση όλων των αποθετηρίων του Leap 42.1 με χρήση του εργαλείου zypper (και φυσικά με δικαιώματα διαχειριστή συστήματος). Το rr αποτελεί συντομογραφία του removerepo και στο παράδειγμα ακολουθείται από τους αύξοντες αριθμούς όλων των υπαρχόντων repositories.



*Το Leap 42.1 χωρίς *κανένα* αποθετήριο :/ Παράξενο θέαμα, ε; Πράγματι είναι παράξενο – και την ίδια στιγμή είναι το πρώτο ουσιαστικό βήμα για την αναβάθμιση στο Leap 42.2.*

Βήμα 3. Θέλουμε τώρα να προσθέσουμε δύο νέα repositories για πακέτα OSS και τις αναβαθμίσεις τους, αλλά για το openSUSE Leap 42.2. Χρειαζόμαστε τα αντίστοιχα URLs κι αυτά είναι ίδια μ' εκείνα που πριν λίγο σημειώσαμε, μόνο που στη θέση του 42.1 υπάρχει το 42.2. Οι προσθήκες επιτυγχάνονται πληκτρολογώντας, διαδοχικά:

```
sub0@vatnajokull:~> sudo zypper ar -n 'openSUSE Leap 42.2 OSS' \
http://mirror.hetzner.de/opensuse/distribution/leap/42.2/repo/oss \
'Leap422 OSS'
sub0@vatnajokull:~> sudo zypper ar -n 'openSUSE Leap 42.2 OSS Updates' \
http://mirror.hetzner.de/opensuse/update/leap/42.2/oss \
'Leap422 OSS Updates'
```



Προσθήκη δύο νέων repositories για τα πακέτα OSS και τις αναβαθμίσεις τους, για το openSUSE Leap 42.2. Η εντολή ar αποτελεί συντομογραφία του addrepo και με την παράμετρο -n καθορίζουμε το όνομα του νέου repository. Ακολουθεί η online διεύθυνσή του και μετά ένα συνώνυμο (alias). Το συνώνυμο ενδέχεται να είναι μια συντομότερη εκδοχή του ονόματος, αν και όχι απαραίτητα.

Βήμα 4. Πριν χρησιμοποιήσουμε τα νέα repositories πρέπει να φρεσκάρουμε την τοπική cache με τις πληροφορίες που τα αφορούν. Αυτό γίνεται πολύ πιο εύκολα απ' όσο ακούγεται, συγκεκριμένα αρκεί να πληκτρολογήσουμε

```
sub0@vatnajokull:~> sudo zypper ref
```

Βήμα 5. Έφτασε η ώρα για το πέρασμα στο Leap 42.2, χρησιμοποιώντας τα δύο repositories που μόλις προσθέσαμε. Πρώτα θα κατεβάσουμε *όλα* τα νέα πακέτα RPM και μετά θα τα εγκαταστήσουμε, οπότε ξεκινάμε δίνοντας:

```
sub0@vatnajokull:~> sudo zypper dup --download-only
```

```
~ — ssh vatnajokull
  libyui7 libyui-ncurses7 libyui-ncurses-pkg7 libz1 libzio1 libzypp logrotate lsof lsscsi lvm2 mailx man man-pages mdadm mkfontdir mkfontscale mozilla-nspr
  mutt nano nano-lang ncurses-utils netcat-openbsd netcfg netpbm net-tools nfsidmap nmap nscd ntp numactl openssh openssh-askpass openssh-helpers openssl
  openSUSE-build-key openSUSE-release openSUSE-release-ftp os-prober p11-kit p11-kit-tools pam pam-config parted patterns-openSUSE-base
  patterns-openSUSE-minimal_base patterns-openSUSE-yast2_basis pciutils pciutils-ids perl perl-base perl-Bootloader perl-Bootloader-YAML perl-Config-Crontab
  perl-Crypt-SmbHash perl-Data-Dump perl-Digest-HMAC perl-Digest-MD4 perl-Digest-SHA1 perl-Encode-Locale perl-File-Listing perl-gettext perl-HTML-Parser
  perl-HTML-Tagset perl-HTML-Tidy perl-HTTP-Cookies perl-HTTP-Daemon perl-HTTP-Date perl-HTTP-Message perl-HTTP-Negotiate perl-IO-HTML perl-IO-Socket-SSL
  perl-libwww-perl perl-LWP-MediaTypes perl-LWP-Protocol-https perl-Net-DBus perl-Net-DNS perl-Net-HTTP perl-Net-SSLeay perl-Parse-RecDescent
  perl-Text-Wrapper perl-Tie-IxHash perl-TimeDate perl-URI perl-WWW-RobotRules perl-X11-Protocol perl-X500-DN perl-XML-LibXML perl-XML-NamespaceSupport
  perl-XML-Parser perl-XML-SAX perl-XML-SAX-Base perl-XML-SAX-Expat perl-XML-Simple perl-XML-Twig perl-XML-XPath perl-XML-XPathEngine perl-YAML-LibYAML
  permissions pigz pinentry pkg-config polkit polkit-default-privs postfix prctl procps psutils pytalloc python python-base python-gobject python-xml
  readline-doc release-notes-openSUSE rpcbind rpm rsync ruby ruby2.1 ruby2.1-rubygem-fast_gettext ruby2.1-rubygem-gem2rpm ruby2.1-rubygem-ruby-dbus
  ruby2.1-stdlib ruby-common samba-client samba-libs samba-winbind sed sed-lang sg3_utils shadow shared-mime-info shared-mime-info-lang shim snapper
  snapper-zypp-plugin strace SuSEfirewall2 suse-module-tools sysconfig sysconfig-netconfig syslinux systemd systemd-bash-completion systemd-logger
  systemd-presets-branding-openSUSE systemd-sysvinit sysvinit-tools tcsh telnet terminfo-base time tmux tnftp traceroute udev unzip unzip-doc
  update-alternatives update-desktop-files urlview util-linux util-linux-lang util-linux-systemd vim vim-data w3m wallpaper-branding-openSUSE wget which
  wireless-regdb wol xauth xbitmaps xdg-utils xfsprogs xtables-plugins xz xz-lang yast2 yast2-add-on yast2-auth-client yast2-bootloader
  yast2-branding-openSUSE yast2-core yast2-country yast2-country-data yast2-firewall yast2-hardware-detection yast2-inetd yast2-installation
  yast2-iscsi-client yast2-journal yast2-ldap yast2-mail yast2-metapackage-handler yast2-network yast2-nfs-client yast2-nfs-common yast2-nis-client
  yast2-ntp-client yast2-online-update yast2-online-update-configuration yast2-online-update-frontend yast2-packager yast2-pam yast2-perl-bindings
  yast2-pkg-bindings yast2-printer yast2-proxy yast2-ruby-bindings yast2-samba-client yast2-samba-server yast2-security yast2-services-manager yast2-slp
  yast2-snapper yast2-storage yast2-sudo yast2-sysconfig yast2-trans-en_US yast2-transfer yast2-trans-stats yast2-tune yast2-update yast2-users yast2-vm
  yast2-xml yast2-ycp-ui-bindings zypper zypper-aptitude zypper-log zypp-plugin-python

The following 3 patterns are going to be upgraded:
  base minimal_base yast2_basis

The following product is going to be upgraded:
  openSUSE

The following 22 packages are going to be downgraded:
  bind-libs bind-utils curl dbus-1 dbus-1-x11 ghostscript ghostscript-x11 libcurl4 libdbus-1-3 libharfbuzz0 libsolv-tools libwicked-0-6 libX11-6 libX11-data
  nfs-client openslp sudo tar tar-lang wicked wicked-service yast2-fonts

The following 7 packages are going to be reinstalled:
  boost-license1_54_0 iscsiuio libarchive13 libboost_system1_54_0 libboost_thread1_54_0 open-iscsi timezone

516 packages to upgrade, 22 to downgrade, 270 new, 7 to reinstall, 8 to remove.
Overall download size: 385.9 MiB. Already cached: 0 B. Download only.
Continue? [y/n/? shows all options] (y):
```

*Αντί να κατεβαίνουν πακέτα και να εγκαθίστανται όπως φτάνουν, προτιμήσαμε να τα κατεβάσουμε πρώτα *όλα* μαζί. Στο παράδειγμά μας, το συνολικό μέγεθος του download ανέρχεται στα 386 περίπου gigabytes.*

Πρακτικά, η προηγούμενη εντολή κατεβάζει όλα τα νέα πακέτα χωρίς να κάνει τίποτε άλλο. Για την αναβάθμιση αυτή καθ' αυτή γράφουμε:

```
sub0@vatnajokull:~> sudo zypper --no-refresh dup
```

Η διαδικασία θα χρειαστεί λίγο χρόνο για να ολοκληρωθεί – στην περίπτωσή μας περισσότερο απ' όσο χρειάστηκε το download.

```
The following 3 patterns are going to be upgraded:
  base minimal_base yast2_basis

The following product is going to be upgraded:
  openSUSE

The following 22 packages are going to be downgraded:
  bind-libs bind-utils curl dbus-1 dbus-1-x11 ghostscript ghostscript-x11 libcurl4 libdbus-1-3 libharfbuzz0 libsolv-tools libwicked-0-6 libX11-6 libX11-data
  nfs-client openslp sudo tar tar-lang wicked wicked-service yast2-fonts

The following 7 packages are going to be reinstalled:
  boost-license1_54_0 iscsiuio libarchive13 libboost_system1_54_0 libboost_thread1_54_0 open-iscsi timezone

516 packages to upgrade, 22 to downgrade, 270 new, 7 to reinstall, 8 to remove.
Overall download size: 0 B. Already cached: 385.9 MiB. After the operation, additional 119.9 MiB will be used.
Continue? [y/n/? shows all options] (y):
```

Ώρα για αναβάθμιση στο openSUSE Leap 42.2! Όλα τα νέα πακέτα έχουν ήδη κατέβει, οπότε τώρα η διαδικασία θα προχωρήσει ομαλότερα και βεβαίως θα ολοκληρωθεί γρηγορότερα.

Μετά το πέρας της, προσέξτε λίγο το τερματικό σας για μηνύματα λάθους. Λογικά όλα θα έχουν πάει καλά και δεν θα εντοπίσετε τίποτε το ανησυχητικό.

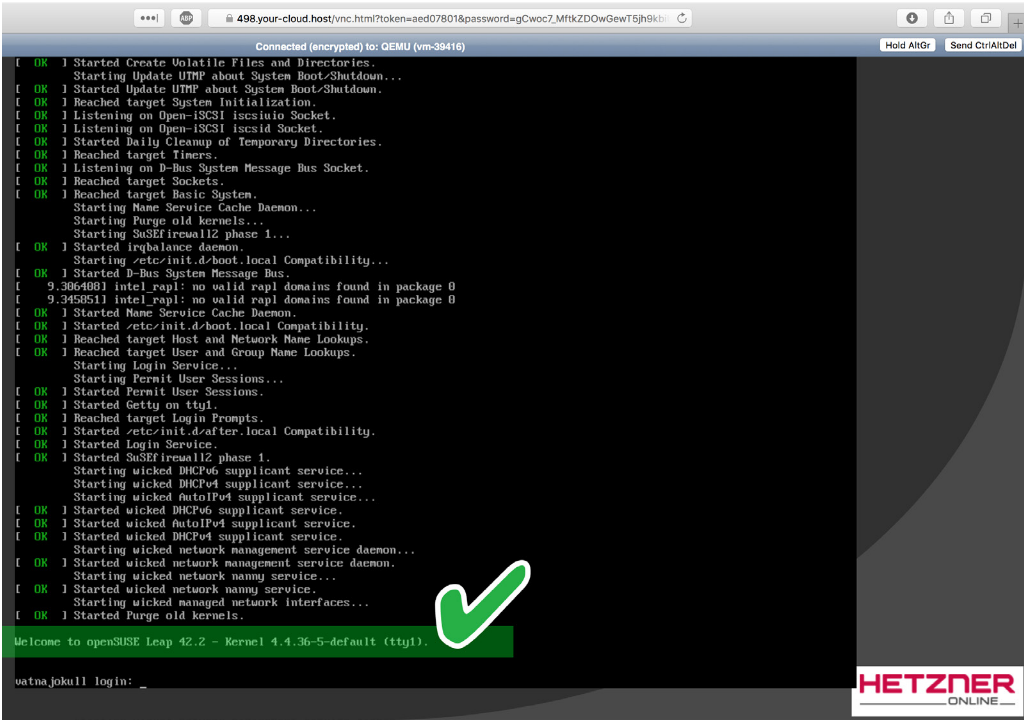
```
~ — ssh vatnajokull
sub0@vatnajokull:~> zypper lr openSUSE-Leap-42.1-Oss
Alias          : repo-oss
Name           : openSUSE-Leap-42.1-Oss
URI            : http://mirror.hetzner.de/opensuse/distribution/leap/42.1/repo/oss/
Enabled        : Yes
GPG Check      : (r ) Yes
Priority       : 99
Auto-refresh   : On
Keep Packages  : Off
Type           : yast2
GPG Key URI    :
Path Prefix    : /
Parent Service :
Keywords       :
Repo Info Path : /etc/zypp/repos.d/repo-oss.repo
MD Cache Path  : /var/cache/zypp/raw/repo-oss
sub0@vatnajokull:~>
sub0@vatnajokull:~> zypper lr openSUSE-Leap-42.1-Update
Alias          : repo-update
Name           : openSUSE-Leap-42.1-Update
URI            : http://mirror.hetzner.de/opensuse/update/leap/42.1/oss/
Enabled        : Yes
GPG Check      : (r ) Yes
Priority       : 99
Auto-refresh   : On
Keep Packages  : Off
Type           : rpm-md
GPG Key URI    :
Path Prefix    : /
Parent Service :
Keywords       :
Repo Info Path : /etc/zypp/repos.d/repo-update.repo
MD Cache Path  : /var/cache/zypp/raw/repo-update
sub0@vatnajokull:~>
```

Η διαδικασία της αναβάθμισης μόλις ολοκληρώθηκε. Όπως βλέπετε και στο screenshot, στο τερματικό μας δεν υπάρχει κάποιο μήνυμα λάθους.

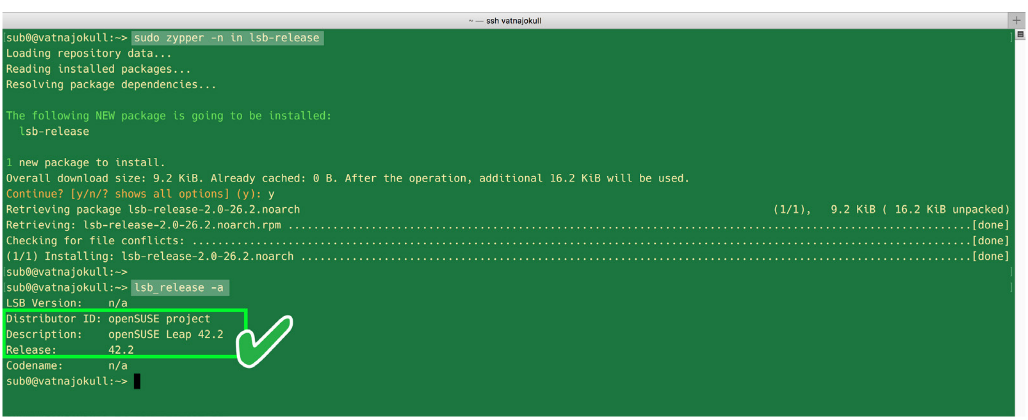
Κάντε μια επανεκκίνηση κι ανοίξτε μια κονσόλα VNC, ώστε να δείτε το μήνυμα καλωσορίσματος πάνω από το login prompt. Θα παρατηρήσετε ότι βρισκόσαστε στο openSUSE Leap 42.2.

Αν ο VPS provider δεν προσφέρει κονσόλα VNC, κάντε SSH login στο απομακρυσμένο σύστημα, εγκαταστήστε το εργαλείο lsb-release (αν δεν είναι ήδη εγκατεστημένο) και δώστε `lsb_release -a`. Καλωσορίσατε στο ολοκαίνουργιο λειτουργικό σας!

Βήμα 6. Κατανοούμε ότι βιάζεστε ν' αρχίσετε τους πανηγυρισμούς και τα πάρτυ, παρακαλούμε όμως, περιμένετε λίγο ακόμα. Έχετε αλήθεια αναρωτηθεί τι ακριβώς συμβαίνει με τα αρχεία ρυθμίσεων εφαρμογών και υπηρεσιών, κάθε φορά που έχουμε αναβάθμιση; Το αρχείο /etc/ssh/sshd_config του OpenSSH, για παράδειγμα, είναι



Μετά την αναβάθμιση στο Leap 42.2 επανεκκινούμε το λειτουργικό και στη web VNC console που μας παρέχεται βλέπουμε τα μηνύματα του boot. Το ξεκίνημα ολοκληρώνεται χωρίς μηνύματα λάθους και, απ' ό,τι υποδηλώνει το μήνυμα πάνω από το login prompt, βρισκόμαστε στο openSUSE Leap 42.2!

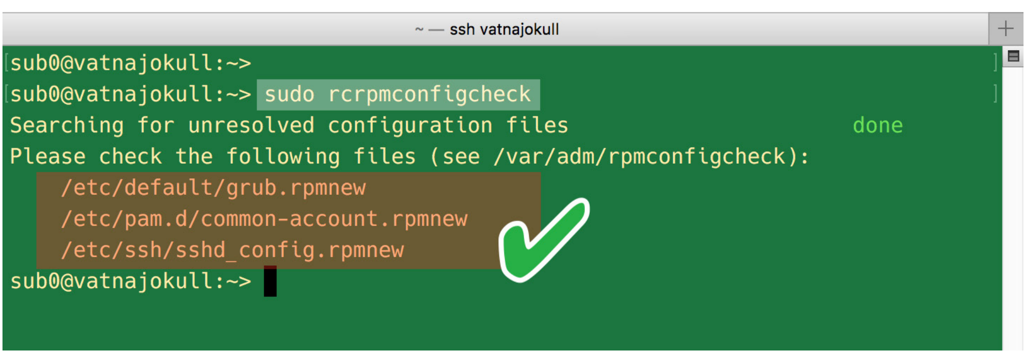


Άλλη μια επιβεβαίωση ότι βρισκόμαστε στο ολοκαίνουργιο Leap 42.2, αυτή τη φορά από το εργαλείο lsb_release.

σχεδόν βέβαιο πως το έχουμε τροποποιήσει. Όταν λοιπόν κατά τη μετάβαση από το Leap 42.1 στο Leap 42.2 αναβαθμίζεται κι ο OpenSSH server (από την έκδοση 1.93 στην 1.98), τι γίνεται με το τροποποιημένο από εμάς sshd_config; Μήπως αντικαθίσταται από το αντίστοιχο αρχείο της νέας έκδοσης, οπότε οφείλουμε να επαναφέρουμε ξανά τις ρυθμίσεις μας από το backup που έχουμε; Όχι ακριβώς. Στην πραγματικότητα, η στρατηγική διαχείρισης των αρχείων ρυθμίσεων έχει ως ακολούθως:

- Αν ένα αρχείο ρυθμίσεων δεν έχει τροποποιηθεί από τον διαχειριστή του συστήματος, τότε απλά αντικαθίσταται από το αντίστοιχο αρχείο της νέας έκδοσης.
- Αν ένα αρχείο ρυθμίσεων έχει τροποποιηθεί από τον διαχειριστή του συστήματος και η αρχική εκδοχή του αρχείου είναι διαφορετική από το αντίστοιχο αρχείο στη νέα έκδοση, τότε στο τροποποιημένο αρχείο προστίθεται η κατάληξη .rpmorig ή .rpmsave κι εγκαθίσταται και το αρχείο της νέας έκδοσης.
- Αν στο αρχείο SPEC του νέου πακέτου που εγκαθίσταται υπάρχει η ετικέτα noreplace, το αρχείο ρυθμίσεων της παλιάς έκδοσης παραμένει ως έχει κι εγκαθίσταται και το αντίστοιχο της νέας έκδοσης, αλλά με την κατάληξη .rpmnew.

Μετά από την αναβάθμιση του λειτουργικού συστήματος αξίζει να αναζητήσουμε αρχεία με καταλήξεις .rpmorig, .rpmsave ή .rpmnew. Προς τούτο, βολικό είναι το εργαλείο rcrpmconfigcheck. Αναλόγως των ευρημάτων μας ίσως απλά σβήσουμε απευθείας τα όποια αρχεία .rpmorig, .rpmsave, .rpmnew έχουμε, ίσως συγχωνεύσουμε αλλαγές μας σε νέα αρχεία και μετά διαγράψουμε τα παλιά. Παρεμπιπτόντως, με το εργαλείο diff είναι πολύ εύκολο να συγκρίνουμε τα περιεχόμενα δύο αρχείων και να εντοπίζουμε τις διαφορές τους.



Μετά την αναβάθμιση στο Leap 42.2 βλέπουμε ότι υπάρχουν τρία αρχεία ρυθμίσεων τα οποία αξίζει να προσέξουμε λίγο. Το sshd_config, παρεμπιπτόντως, είναι ένα από τα αρχεία που πάντα τροποποιούμε (απαγόρευση απομακρυσμένου login στο λογαριασμό του root, απαγόρευση authentication με βάση το password, authentication μόνο με βάση τα κλειδιά SSH).

```
~ — delta@thesender: ~/lists — ssh vatnajokull
1c1
< #     $OpenBSD: sshd_config,v 1.93 2014/01/10 05:59:19 djm Exp $
---
> #     $OpenBSD: sshd_config,v 1.98 2016/02/17 05:29:04 djm Exp $
28a29,33
> # Minimum accepted size of the DH parameter p. By default this is set to 1024
> # to maintain compatibility with RFC4419, but should be set higher.
> # Upstream default is identical to setting this to 2048.
> #KexDHMin 1024
>
44c49
< PermitRootLogin no
---
> #PermitRootLogin yes
50c55
< PubkeyAuthentication yes
---
> #PubkeyAuthentication yes
76c81
< ChallengeResponseAuthentication no
---
> #ChallengeResponseAuthentication yes
90,95d94
< # Set this to 'yes' to enable support for the deprecated 'gssapi' authentication
< # mechanism to OpenSSH 3.8p1. The newer 'gssapi-with-mic' mechanism is included
< # in this release. The use of 'gssapi' is deprecated due to the presence of
< # potential man-in-the-middle attacks, which 'gssapi-with-mic' is not susceptible to.
< #GSSAPIEnableMITMAttack no
<
118c117
< UsePrivilegeSeparation sandbox                # Default for new installations.
---
> #UsePrivilegeSeparation sandbox
123c122
< #UseDNS yes
---
lines 1-36
```

Χρήση του diff για τον εντοπισμό των διαφορών μεταξύ των αρχείων sshd_config και sshd_config.rpmnew.

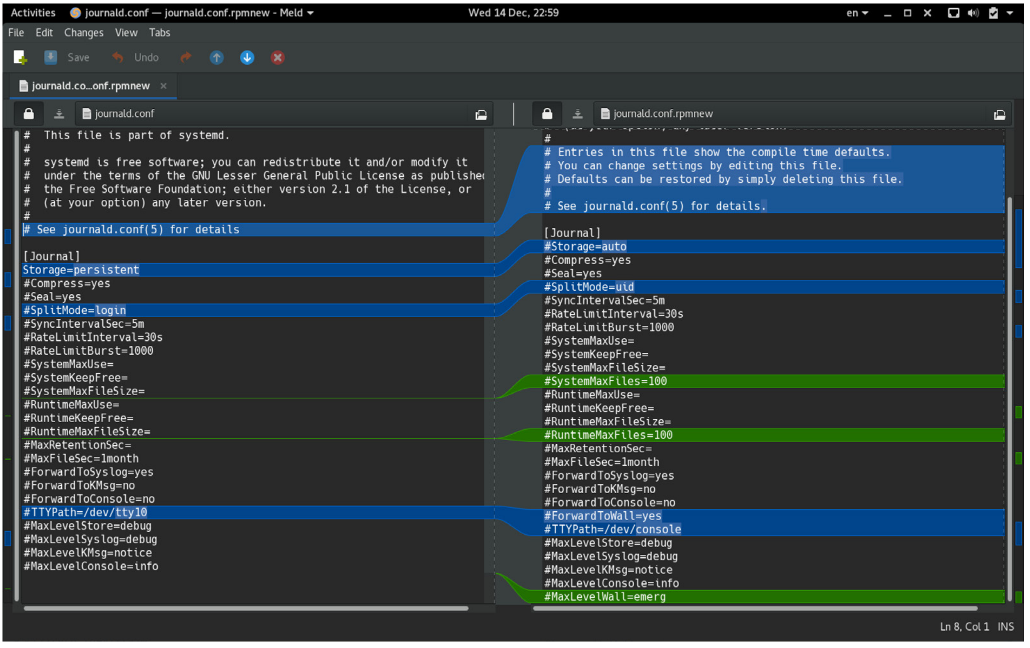
Αναβάθμιση συστήματος desktop, από τη γραμμή εντολών

Όπως ήδη αναφέραμε, με εντελώς παρόμοιο τρόπο μπορούμε να εργαστούμε προκειμένου ν' αναβαθμίσουμε ένα σύστημα desktop με openSUSE Leap 42.1. Σε σχέση με τη διαδικασία αναβάθμισης του VPS, με το desktop υπάρχουν δύο μόνο σημεία που χρειάζονται προσοχή:

Πέρα από τα repositories OSS και OSS Updates της έκδοσης 42.2, θα χρειαστεί να προσθέσουμε και τα repositories Non OSS και Non OSS Updates — πάντα της έκδοσης 42.2.

Μετά την αναβάθμιση του λειτουργικού κατά πάσα πιθανότητα θα χρειαστεί να προσθέσουμε και τα όποια έξτρα repositories χρησιμοποιούσαμε προηγουμένως (και κατά νου έχουμε κυρίως το Packman repository).

Περισσότερες λεπτομέρειες δεν θα παραθέσουμε, είμαστε βέβαιοι ότι δεν τις χρειαζόσαστε.



Αν η έξοδος του εργαλείου diff σας φαίνεται κάπως δυσνόητη, εντοπίστε τις διαφορές μεταξύ δύο αρχείων καταφεύγοντας στην εφαρμογή ονόματι meld. Αν το meld δεν είναι ήδη παρόν στο σύστημά σας, εγκαταστήστε το με το zypper.

Skill: Intermediate
Tags: Raspberry Pi, Raspbian, Apache, Let's Encrypt

Ο Apache στο Raspberry Pi, με έγκυρο πιστοποιητικό

Μεταξύ των αναρίθμητων πρότζεκτ που μπορούμε να υλοποιήσουμε γύρω από το Raspberry Pi, πολλά απαιτούν την παρουσία web server. Στο παρόν άρθρο εγκαθιστούμε τον Apache, ενώ αμέσως μετά δείχνουμε και πώς αποκτούμε δωρεάν πιστοποιητικό για το site που σερβίρει.

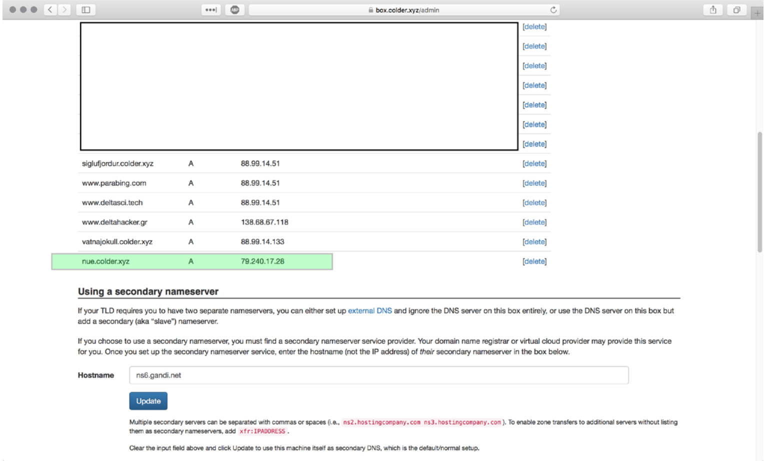
Ναι, ακόμη και για το site που φιλοξενείται στο Raspberry Pi μας στο σπίτι, είναι πράγματι δυνατόν να πάρουμε ένα έγκυρο πιστοποιητικό από το Let's Encrypt (https://letsencrypt.org) κι έτσι όλοι οι επισκέπτες να απολαμβάνουν έμπιστες κι ασφαλείς συνδέσεις HTTPS. Πριν ξεκινήσουμε με την όλη διαδικασία φροντίζουμε ώστε να έχουμε:

- **Ένα Raspberry Pi,** κατά προτίμηση το 3 model B, με το Raspbian εγκατεστημένο και ρυθμισμένο. Περισσότερα επ' αυτού μπορείτε να διαβάσετε στο https://deltahacker.gr/raspbian-on-raspi. Αντί για το Raspbian μπορείτε βεβαίως να χρησιμοποιείτε κάποια άλλη διανομή Linux. Να σημειώσουμε ότι η παρουσίασή μας δεν ισχύει μόνο για το Raspbian, υπόψιν όμως ότι ενέργειες όπως είναι η εγκατάσταση πακέτων ή η διαχείριση υπηρεσιών ίσως γίνονται με διαφορετικό τρόπο σε άλλες διανομές. Ανάλογη παρατήρηση οφείλουμε να κάνουμε και για τις θέσεις των configuration files.
- **Static IP mapping** στον router μπροστά από το Raspberry Pi (στο εξής RasPi), ώστε η συσκευή να παίρνει πάντοτε την ίδια διεύθυνση IP. Αν ο router δεν υποστηρίζει static IP mapping, ρυθμίζουμε το Raspbian ώστε αντί να ζητάει διεύθυνση IP από τον όποιο DHCP server να χρησιμοποιεί πάντοτε το ίδιο IP. Φυσικά, το εν λόγω IP θα πρέπει να έχει νόημα για το LAN εντός του οποίου βρίσκεται το RasPi και να μην είναι ένα από εκείνα που αυτόματα μοιράζει ο DHCP server.
- **Κανόνες port forwarding** στον router, ώστε όποιος επιχειρεί σύνδεση σε κάποιο από τα ports 80/TCP και 443/TCP στο WAN interface του router, να ανακατευθύνεται στο αντίστοιχο port του network interface του RasPi. Πιο συγκεκριμένα, αναφερόμαστε σ' εκείνο το network interface του RasPi που βλέπει απευθείας το LAN interface του router. Στο Raspberry Pi 3 των δοκιμών μας, για παράδειγμα, από τα δύο network interfaces που διαθέτει εκείνο που βλέπει

απευθείας το LAN interface του router είναι το ενσύρματο (κι όχι το ασύρματο). Εναλλακτικά, αντί για κανόνες port forwarding μπορούμε να βάλουμε το RasPi στο DMZ του router. Σε κάθε περίπτωση, το firewall του router ή/και του RasPi οφείλουμε να το έχουμε έτσι ρυθμισμένο, ώστε ειδικά στους clients από το Internet να επιτρέπεται πρόσβαση *μόνο* σε ένα σαφώς ορισμένο σύνολο υπηρεσιών. Το RasPi μας δεν είναι στο DMZ, το firewall του router είναι ενεργοποιημένο και, χάρη σε τρεις κανόνες port forwarding, για τους clients από το Internet γίνονται ανακατευθύνσεις *μόνο* προς τα ports των υπηρεσιών SSH, HTTP και HTTPS του RasPi. Στο ίδιο το RasPi δεν υπάρχει firewall ενεργοποιημένο, αφού δεν ανησυχούμε για τους χρήστες του τοπικού δικτύου.

- **Το δικό μας domain name** και πρόσβαση στον name server που το φιλοξενεί. Στον name server πρέπει να υπάρχει ένα A record για το domain ή κάποιο subdomain του, το οποίο θα δείχνει στο δημόσιο IP του router μπροστά από το RasPi (περισσότερα για το DNS και τους name servers μπορείτε να διαβάσετε στο https://deltahacker.gr/?p=14749). Βεβαίως, επειδή το IP αυτό μάλλον δεν θα είναι στατικό και θ' αλλάζει, οφείλουμε να φροντίσουμε για έναν μηχανισμό που θα ενημερώνει αυτόματα το A record. Εμείς έχουμε στην κατοχή μας το domain colder.xyz, το οποίο εξυπηρετείται από τον name server μιας εγκατάστασης του Mail-in-a-Box (https://deltahacker.gr/?p=14096). Για τις ανάγκες του παρόντος άρθρου, στον name server προσθέσαμε ένα A record το οποίο στο subdomain nue.colder.xyz αντιστοιχίζει το δημόσιο IP που παίρνει ο router μας από τον ISP. Στο δε Raspbian υπάρχει ένα cronjob που κάθε μισή ώρα ενημερώνει κατάλληλα το A record του name server. Αλλά δείτε τα screenshots που ακολουθούν, διαβάστε και τις αντίστοιχες περιγραφές.

Σημείωση. Αν δεν έχετε το δικό σας domain ή δεν είναι δυνατή η αυτόματη ενημέρωση των A records του name server, στραφείτε προς κάποια (δωρεάν) υπηρεσία dynamic DNS. Μια από τις επιλογές σας είναι η σχετική υπηρεσία του Duck DNS (https://www.duckdns.org).



Όψη του web panel που διαθέτει η εγκατάσταση του Mail-in-a-Box μας, την οποία συντηρούμε σε VPS της Digital Ocean. Ο name server εξυπηρετεί περισσότερα από ένα domains, μεταξύ αυτών και το colder.xyz. Παρατηρήστε το A record για το subdomain nue.colder.xyz, το οποίο δείχνει προς το δημόσιο IP του router μπροστά από το RasPi.



Το συγκεκριμένο cronjob του RasPi κάθε μισή ώρα ενημερώνει κατάλληλα το A record για το subdomain nue.colder.xyz, ώστε πάντοτε να εμπεριέχει τη δημόσια δυναμική διεύθυνση IP που παίρνει ο router μας από τον ISP.

Εγκατάσταση Apache

Συνδεόμαστε μέσω SSH στο RasPi κι αρχικά φροντίζουμε ώστε οι πληροφορίες περί των αποθετηρίων να είναι επικαιροποιημένες:

```
pi@nordostbahnhof:~ $ sudo apt-get update
```

Ακολούθως εγκαθιστούμε τον Apache:

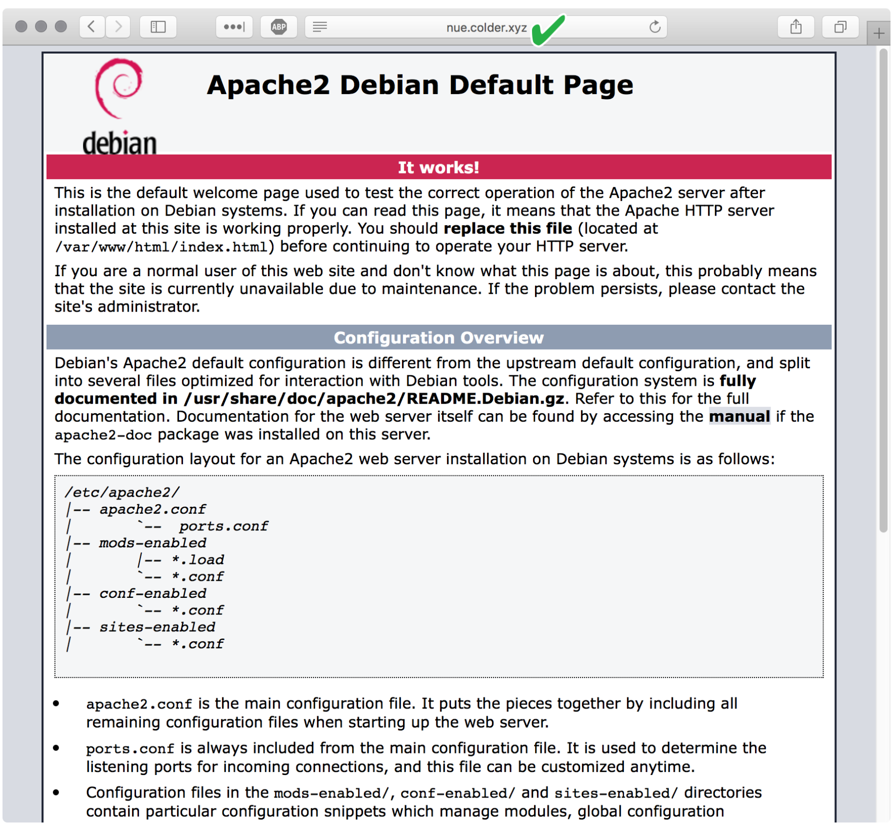
```
pi@nordostbahnhof:~ $ sudo apt-get -y install apache2
```

Όπως εύκολα διαπιστώνουμε, αμέσως μετά την εγκατάστασή του ο web server είναι ενεργοποιημένος:

```
pi@nordostbahnhof:~ $ sudo systemctl -l status apache2
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─forking.conf
   Active: active (running) since Sat 2016-12-24 08:03:02 CET; 1min 21s ago
   CGroup: /system.slice/apache2.service
           ├─18621 /usr/sbin/apache2 -k start
           ├─18624 /usr/sbin/apache2 -k start
           └─18625 /usr/sbin/apache2 -k start
```

```
Dec 24 08:03:01 nordostbahnhof apache2[18598]: Starting web server:
apache2AH00558: apache2: Could not reliably determine the server's fully
qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally
to suppress this message
Dec 24 08:03:02 nordostbahnhof apache2[18598]: .
Dec 24 08:03:02 nordostbahnhof systemd[1]: Started LSB: Apache2 web server.
```

Υπάρχουν κάποια παράπονα περί FQDN (fully qualified domain name) τα οποία μπορούμε να αγνοήσουμε επιδεικτικά — αν και μάλλον είναι ήδη αργά γι' αυτό :/ Από έναν οποιονδήποτε web browser επισκεπτόμαστε τη διεύθυνση της μορφής http://στατικό_εσωτερικό_IP_του_RasPi ή της μορφής http://το_(sub)domain_μας. Παράδειγμα: Το στατικό IP του δικού μας RasPi είναι το 192.168.178.31 και το subdomain μας είναι το nue.colder.xyz, επομένως από τον web browser πηγαίνουμε σε ένα από τα http://192.168.178.31, http://nue.colder.xyz (φυσικά, καλό είναι να τσεκάρουμε και τις δύο διευθύνσεις). Σε κάθε περίπτωση, αν όλα έχουν πάει καλά με τον Apache θα δούμε την προκαθορισμένη του σελίδα, με πληροφορίες που τον αφορούν.



Η σελίδα καλωσορίσματος του Apache, αμέσως μετά την εγκατάστασή του στο RasPi μας. Παρατηρήστε ότι επισκεφτήκαμε το σχετικό site με χρήση του subdomain μας, δηλαδή όπως ακριβώς θα έκανε ένας οποιοσδήποτε χρήστης του Internet.

Εγκατάσταση Let's Encrypt client

Ο προαναφερθείς client δεν υπάρχει στα repositories του Raspbian και γι' αυτό θα τον εγκαταστήσουμε κλωνοποιώντας το σχετικό πρότζεκτ από το GitHub. Για τη συνέχεια βολεύει να εργαστούμε από το λογαριασμό του root:

```
pi@nordostbahnhof:~ $ sudo su
root@nordostbahnhof:~# cd
```

Για την κλωνοποίηση χρειαζόμαστε το git:

```
root@nordostbahnhof:~# apt-get -y install git
```

Ο προσωπικός κατάλογος του root είναι ένα καλό σημείο για την κλωνοποίηση του Let's Encrypt client:

```
root@nordostbahnhof:~# git clone https://github.com/letsencrypt/letsencrypt
Cloning into 'letsencrypt'...
remote: Counting objects: 42706, done.
remote: Compressing objects: 100% (167/167), done.
remote: Total 42706 (delta 85), reused 4 (delta 4), pack-reused 42529
Receiving objects: 100% (42706/42706), 12.16 MiB | 2.67 MiB/s, done.
Resolving deltas: 100% (30440/30440), done.
Checking connectivity... done.
```

Ωραία, είμαστε τώρα έτοιμοι να αιτηθούμε πιστοποιητικό για το domain ή/και για τα subdomain μας.

Λήψη πιστοποιητικού

Προηγουμένως δημιουργήθηκε ο κατάλογος ονόματι letsencrypt. Μεταβαίνουμε σ' αυτόν...

```
root@nordostbahnhof:~# cd letsencrypt
```

...κι εγκαθιστούμε ένα ωραιότατο πιστοποιητικό για τον Apache πληκτρολογώντας κάτι σαν το ακόλουθο:

```
root@nordostbahnhof:~/letsencrypt# ./letsencrypt-auto --apache -d nue.colder.
xyz -m subZraw@colder.xyz --redirect --agree-tos
```

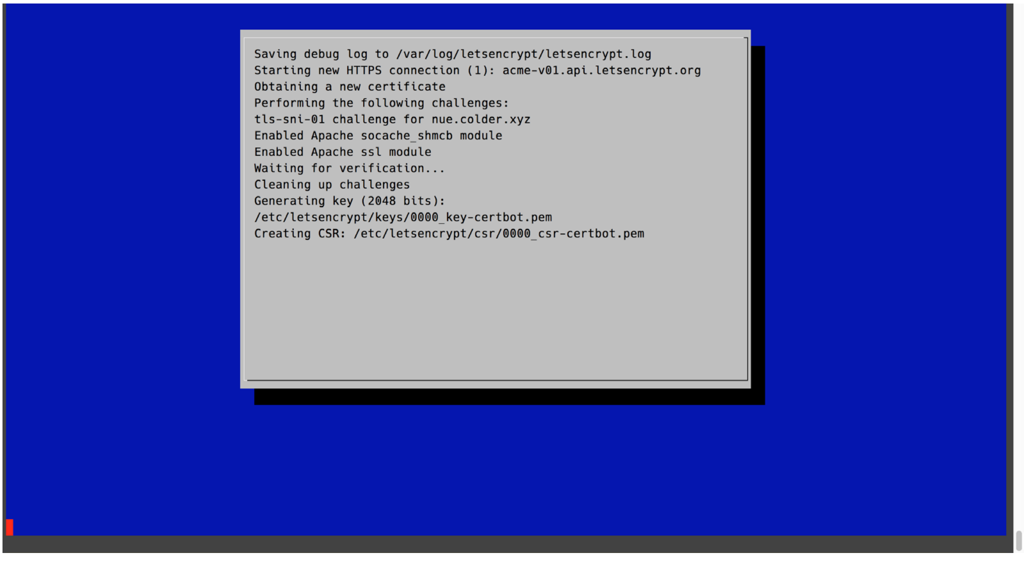
Με την παράμετρο -d ορίζουμε το domain ή το subdomain για το οποίο αιτούμαστε πιστοποιητικό. Αν ζητάμε πιστοποιητικό που να καλύπτει ένα domain κι ένα ή περισσότερα subdomains του, απλά χρησιμοποιούμε την παράμετρο -d περισσότερες από μία φορές. Για παράδειγμα, αν θέλαμε πιστοποιητικό που να καλύπτει το site του περιοδικού, τότε θα γράφαμε:

```
root@nordostbahnhof:~/letsencrypt# ./letsencrypt-auto --apache -d deltahacker.
gr -d www.deltahacker.gr -m talk2us@deltahacker.gr --redirect --agree-tos
```

Παρατηρήστε την παράμετρο -m, η οποία δέχεται μια έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου. Σ' αυτή τη διεύθυνση αποστέλλονται emails με έγκαιρες ειδοποιήσεις από το Let's Encrypt πρότζεκτ, κάθε φορά που ένα πιστοποιητικό μας πρόκειται να λήξει.

Ιδιαίτερα χρήσιμη, εξάλλου, είναι η επιλογή --redirect. Όταν τη συμπεριλαμβάνουμε στην εντολή αίτησης πιστοποιητικού, τα αρχεία ρυθμίσεων του Apache τροποποιούνται καταλλήλως ώστε ασχέτως αν οι επισκέπτες πληκτρολογούν http://domain.tld ή https://domain.tld, πάντα να χρησιμοποιούν την ασφαλή σύνδεση HTTPS.

Αφού λοιπόν πληκτρολογήσουμε την κατάλληλη εντολή, οι διαδικασίες αίτησης πιστοποιητικού, ελέγχου ιδιοκτησιακού καθεστώτος του αντίστοιχου domain, εγκατάστασης πιστοποιητικού κι ενημέρωσης του Apache, προχωρούν κι ολοκληρώνονται αυτόματα. Δείτε τα screenshots που ακολουθούν.



Στο σκριπτάκι letsencrypt-auto δώσαμε την παράμετρο --apache κι ο client ξέρει πώς να τροποποιεί τα configuration files του εν λόγω web server, οπότε δεν χρειάζεται καμία επέμβαση από μέρους μας. Μεταξύ των άλλων εργασιών που επιτελούνται αυτόματα είναι κι ο έλεγχος ιδιοκτησίας του domain name. Την πρόοδο των εργασιών την παρακολουθούμε μέσα από ένα απλό αλλά επεξηγηματικό ncurses interface.

```
Congratulations! You have successfully enabled
https://nue.colder.xyz

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=nue.colder
.xyz

                    < OK >
```

Η εγκατάσταση του πιστοποιητικού ολοκληρώθηκε επιτυχώς για το nue.colder.xyz! Παροτρυνόμαστε να πάμε μια βόλτα από το https://ssllabs.com για μια σειρά από ελέγχους ασφαλείας. Θα το κάνουμε, αλλά σε λίγο.

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/nue.colder.xyz/fullchain.pem. Your cert will
   expire on 2017-03-24. To obtain a new or tweaked version of this
   certificate in the future, simply run letsencrypt-auto again with
   the "certonly" option. To non-interactively renew *all* of your
   certificates, run "letsencrypt-auto renew"
 - If you lose your account credentials, you can recover through
   e-mails sent to subZraw@colder.xyz.
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

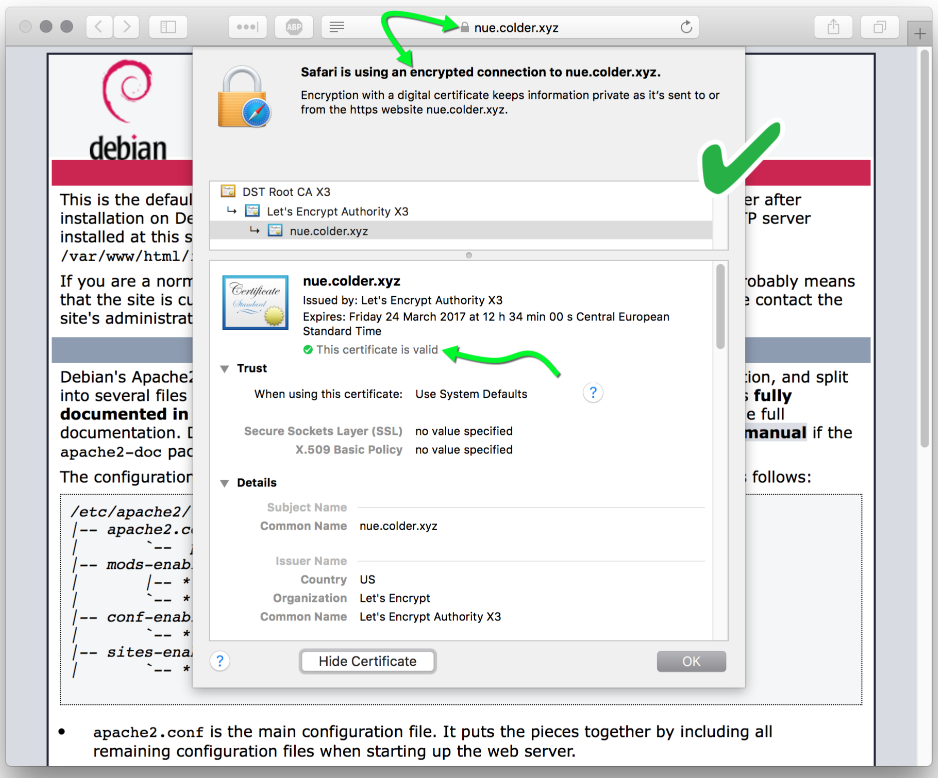
   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

root@nordostbahnhof:~/letsencrypt#
```

*Στις πληροφορίες που επιστρέφει το letsencrypt-auto συμπεριλαμβάνεται και σύντομη οδηγία για την ανανέωση του πιστοποιητικού, αφού εξ ορισμού έχει χρόνο ισχύος τριών μηνών μόνο. Σε λίγο θα φτιάξουμε ένα νέο cronjob ώστε η ανανέωση να γίνεται έγκαιρα κι αυτόματα, κι έτσι το πιστοποιητικό του site μας να είναι *πάντοτε* έγκυρο.*

Απαραίτητοι έλεγχοι

Η διαδικασία έως τώρα ήταν τόσο απλή, σε βαθμό που κάποιοι πιθανώς να σκεφτούν ότι κάτι δεν πήγε καλά. Κι όμως, ο Apache έχει πλέον το έγκυρο πιστοποιητικό του και για να βεβαιωθούμε αρκεί να πάμε στον web browser της προτίμησής μας και να επισκεφτούμε το site.

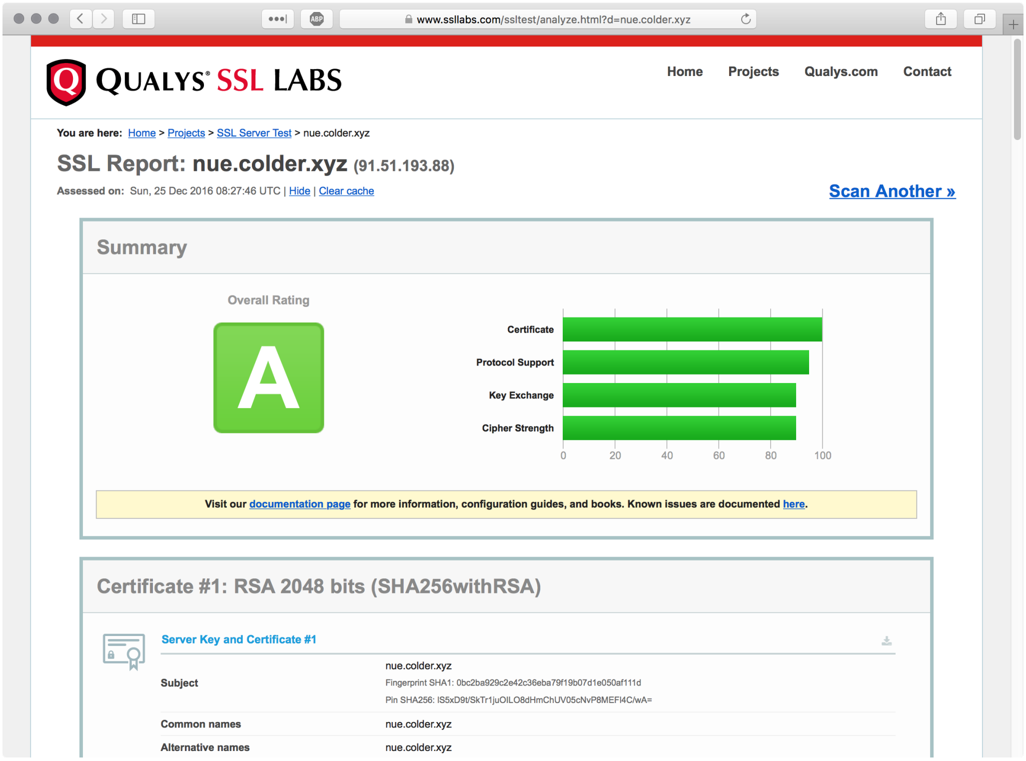


Στη μπάρα διευθύνσεων του web browser πληκτρολογούμε τη διεύθυνση https://nue.colder.xyz (https, όχι απλά http). Η προκαθορισμένη σελίδα του Apache εμφανίζεται και με κλικ πάνω στο εικονίδιο με το λουκέτο παίρνουμε πληροφορίες για το πιστοποιητικό του site. Όλα δείχνουν καλά – και είναι καλά!

Πριν λίγο, όταν ολοκληρώθηκε η διαδικασία εγκατάστασης του πιστοποιητικού, ο client του Let's Encrypt μάς πρότεινε να πάμε στη διεύθυνση

https://www.ssllabs.com/ssltest/analyze.html?d=nue.colder.xyz&latest

ώστε να διεξαχθούν μια σειρά από δοκιμές αναφορικά με την ποιότητα των συνδέσεων SSL (HTTPS) που υποστηρίζει ο web server του nue.colder.xyz. Έχει έρθει η στιγμή να κάνουμε κι αυτές τις δοκιμές και, περιττό να σημειώσουμε, ότι στη θέση του nue.colder.xyz εσείς θα βάλετε το domain name (ή το subdomain) σας.



*Οι έλεγχοι του SSL server (ο Apache μας!) διαρκούν μερικά λεπτά και μετά παίρνουμε μια αξιολόγηση για την ποιότητα των συνδέσεων HTTPS που υποστηρίζει ο διακομιστής. Η τελική βαθμολογία διαμορφώνεται από δεκάδες παραμέτρους κι όπως βλέπετε πήραμε ένα ωραιότατο "A". Αν όλα έχουν πάει καλά, αυτή τη βαθμολογία *τουλάχιστον* θα πρέπει να δείτε και για τον δικό σας SSL server. Υπόψιν ότι υπάρχει και καλύτερη βαθμολογία (A+). Το πώς μπορούμε να την κερδίσουμε ξεφεύγει από τους σκοπούς του παρόντος.*

Αυτόματη ανανέωση πιστοποιητικού

Τα πιστοποιητικά που εκδίδει το Let's Encrypt διαρκούν για τρεις μήνες. Από εκεί και πέρα, αν δεν έχουμε φροντίσει για την ανανέωση του δικού μας, οι επισκέπτες του site βλέπουν τη γνωστή, ανησυχητική προειδοποίηση περί ληγμένου πιστοποιητικού. Ευτυχώς η ανανέωσή τους υποστηρίζεται από τον Let's Encrypt client, οπότε μπορούμε να φτιάξουμε ένα cronjob για τον root που θα φροντίζει γι' αυτή τη δουλειά αυτόματα. Από το λογαριασμό του root, λοιπόν, πληκτρολογούμε

```
root@nordostbahnhof:~/letsencrypt# crontab -e
```

και προσθέτουμε μια νέα εργασία για τον cron daemon. Δείτε τη δική μας:

```
15 4 * * 5 /root/letsencrypt/letsencrypt-auto renew >> /var/log/letsencrypt/
ltenc-renew.log
```

Κάθε Παρασκευή στις 04:15 το πρωί καλείται το letsencrypt-auto με την εντολή renew. Αν και μόνον αν το πιστοποιητικό μας πλησιάζει στη λήξη του, τότε ανανεώνεται αυτόματα. Αν κάτι δεν πάει καλά και χρειαστεί να δούμε τι συνέβη με την απόπειρα ανανέωσης, θα ανοίξουμε το αρχείο /var/log/letsencrypt/ltenc-renew.log. Και μια τελευταία σημείωση: Καλό είναι να βάλετε διαφορετική μέρα και ώρα στο cronjob σας, ώστε να μην ενοχλούμε όλοι μαζί τους servers του Let´s Encrypt. Ας τους ενοχλούμε κατά υποομάδες και πιο τυχαία, δηλαδή :)



Τα cronjobs που είναι σε ισχύ για τον χρήστη root, στο Raspbian. Με το δεύτερο φροντίζουμε για την έγκαιρη ανανέωση του πιστοποιητικού που έχουμε πάρει από το Let's Encrypt.